دليل إدارة خواديم أوبنتو

الإصدار 14.04

ubuntu

عبد اللطيف ايمش

دليل إدارة خواديم أوبنتو

الإصدار 14.04

ترجمة

عبد اللطيف ايمش



عبد اللطيف ايمش

عبد اللطيف ايمش، أدرس الهندسة المدينة في جامعة حلب، مهتم بالتقنية خصوصًا تطوير الويب وإدارة الأنظمة والخواديم؛ مترجم كتاب «سطر أوامر لينُكس» وشاركت في تأليف كتاب «تعلم البرمجة بلغة PHP».

أكتب حاليًا في أكاديمية حسوب، ويمكنك التواصل معي عبر بريدي الإلكتروني: abdallatif.ey@gmail.com.

هذا الكتاب

أُنتج هذا الكتاب برعاية شركة حسوب وأكاديمية حسوب.



أكاديمية حسوب

تهدف أكاديمية حسوب إلى توفير مقالات ودروس عالية الجودة حول مجالات مُختلفة وبلغة عربية فصيحة. باب المُساهمة على الأكاديمية مفتوح لكل من يرى في نفسه القدرة على توفير مقالات عالية الجودة.

Academy.hsoub.com

شركة حسوب

تهدف حسوب لتطوير الويب العربي وخدمات الإنترنت عن طريق توفير حلول عملية وسهلة الاستخدام لتحديات مختلفة تواجه المستخدمين في العالم العربي. يعمل في حسوب فريق شاب وشغوف من مختلف الدول العربية وتمتلك الشركة عدة خدمات يمكن معرفتها بزيارة موقع الشركة

Hsoub.com

الفهرس

تقديم

رافقت زيادة استخدام شبكة الإنترنت زيادةً كبيرةً في عدد الحواسيب التي تعمل مخدماتٍ لمختلف الخدمات الشائعة، كمواقع الويب والبريد الإلكتروني والمراسلة الفورية وخواديم الملفات وخلافه؛ وقد أثبت نظام لينُكس Linux تفوقه في مجال الخواديم، وخصوصًا بعد الانتشار الواسع لتوزيعة أوبنتو الخاصة بالخواديم؛ الذي يُعنى هذا الدليل بشرح طرق تثبيت وضبط مختلف خدماتها.

لذا جاء هذا الكتاب كترجمة للدليل الرسمي لإدارة أوبنتو للخواديم «Ubuntu Server Guide». آمل أن يكون إضافةً مفيدةً للمكتبة العربية؛ وأن يفيد القارئ العربي في تعلم إدارة أحد أشهر نُظم تشغيل الخواديم. والله وليُّ التوفيق.

عبد اللطيف محمد أديب ايمش

٢٠١٦\١\١١

حلب، سورية

١

تمهيد

أهلًا بك في دليل إدارة خواديم أوبنتو! ستجد هنا معلوماتٍ حول تثبيت وإعداد مختلف تطبيقات الخادوم؛ يوضح هذا الدليل طريقة إجراء المهام لتهيئة وتخصيص نظامك خطوةً بخطوة.

يفترض هذا الدليل أنك على درايةٍ أساسيةٍ بنظام أوبنتو، بعض معلومات التثبيت مغطاةٌ في «الفصل الثاني: التثبيت»؛ لكن إذا أردت تعليماتٍ تفصيليةً عن تثبيت أوبنتو، فالرجاء مراجعة «دليل تثبيت أوبنتو».

١. الدعم

هنالك طريقتان تُدعَم فيهما نسخة الخادوم من أوبنتو: الدعم التجاري، ودعم المجتمع؛ حيث أن الدعم التجاري الرئيسي (وتمويل التطوير) متوفر من شركة كانونيكال (Canonical Ltd.)، حيث يوفرون عقود دعمٍ ذات سعرٍ مقبول على كل حاسوب مكتبي، أو على كل الخادوم. راجع صفحة «خدمات كانونيكال» لمزيدٍ من المعلومات.

دعم المجتمع متوفر أيضًا من أشخاص متفرغين وشركات، الذين يأملون أن تكون أوبنتو أفضل توزيعة ممكنة، يُوفَّر الدعم عبر عدّة قوائم بريدية، وقنوات IRC، والمنتديات، والمدونات، وكذلك ويكي ... إلخ. يمكن أن تكون الكمية الكبيرة من المعلومات مُشَتِّتة، لكن يمكن لعبارة بحث جيدة في محرك البحث أن توفر إجابةً لأسئلتك، راجع صفحة «دعم أوبنتو» لمزيدٍ من المعلومات.

٢

التثبيت

يوفر هذا الفصل لمحةً عامةً سريعةً عن تثبيت نسخة الخادوم من أوبنتو ١٤.٠٤، للمزيد من المعلومات المفصّلة، رجاءً راجع «دليل تثبيت أوبنتو».

ا. التحضير للتثبيت

يشرح هذا القسم النواحي المختلفة التي يجب أن تؤخذ بعين الاعتبار قبل البدء بالتثبيت.

ا. متطلبات النظام

تدعم نسخة الخادوم من أوبنتو ١٤.٠٤ ثلاث معماريات رئيسية: إنتل x86، و AMD64، و ARM؛ يعرض الجدول الآتي مواصفات العتاد المستحسنة؛ لكن اعتمادًا على استخدامك للنظام، ربما يمكنك تشغيل النظام بأقل من هذه المواصفات، لكن لا ينصح أبدًا بتجاهل هذه الاقتراحات.

الجدول ٢-١: مواصفات العتاد المستحسنة

نوع التثبيت	المعالج	الذاكرة العشوائية	مساحة القرص الصلب	
			أساس النظام	جميع المهام مثبتة
خادوم (قياسي)	١ غيغاهرتز	٥١٢ ميغابايت	١ غيغابايت	١.٧٥ غيغابايت
خادوم (الحد الأدنى)	٣٠٠ ميغاهرتز	١٩٢ ميغابايت	٧٠٠ ميغابايت	١.٤ غيغابايت

توفر نسخة الخادوم أساسًا مشتركًا لجميع أنواع برمجيات الخادوم، حيث تمثل تصميمًا مصغرًا يوفر منصةً للخدمات المطلوبة، كخدمات مشاركة الملفات أو الطابعات، أو استضافة مواقع الويب، أو البريد الإلكتروني ...إلخ.

ب. الاختلافات بين نسختي الخادوم وسطح المكتب

هنالك بعض الاختلافات بين نسخة الخادوم وسطح المكتب في أوبنتو، عليك أن تلحظ أن كلا النسختين تَستخدمان مستودعات apt نفسها، مما يجعل من السهل تثبيت تطبيق من تطبيقات الخادوم على نسخة سطح المكتب، وكذلك هو الحال في نسخة الخادوم.

تكمن الاختلافات بين النسختين في عدم وجود بيئة النوافذ X في نسخة الخادوم، بالإضافة إلى عملية التثبيت، وخيارات النواة المختلفة.

ج. اختلافات النواة

في أوبنتو ١٠.١٠ وما قبلها، كان لنسختي الخادوم وسطح المكتب أنوية مختلفة؛ لكن أوبنتو لم تعد تفصل الأنوية الخاصة بالخواديم والأنوية الشاملة (generic)، حيث دمجتا في نواة شاملة واحدة لتقليل عبء صيانة النواة طوال فترة دعم الإصدارة.

ملاحظة: عندما تُشغِّل نسخة ٦٤ بت من أوبنتو على معالجات ٦٤ بت، فلن تكون محدودًا بسعة عناوين الذاكرة.

لرؤية جميع إعدادات خيارات النواة، ألق نظرةً على /boot/config-3.13.0-server، وأيضًا على كتاب «Linux Kernel in a Nutshell» الذي هو مصدر رائع للمعلومات حول الخيارات المتوفرة.

د. النسخ الاحتياطي

يجدر بك قبل تثبيت نسخة الخادوم من أوبنتو أن تتأكد أنَّ جميع البيانات على الخادوم قد نُسِخَت احتياطيًا، راجع «الفصل التاسع عشر: النسخ الاحتياطي»؛ لخيارات النسخ الاحتياطي.

إذا لم تكن هذه أول مرة يُثبَّت فيها نظام تشغيل على حاسوبك، فربما عليك إعادة تقسيم القرص الصلب لإيجاد مساحة فارغة لتثبيت أوبنتو عليها.

في أي وقت تعيد فيه تقسيم قرصك الصلب، كن مستعدًا لأن تخسر جميع البيانات عليه في حال ارتكبت خطأً أو حدث شيء ما بشكل خاطئ أثناء التقسيم؛ وذلك على الرغم من أنَّ البرامج المستخدمة في التثبيت عملية جدًا وثابتة ومَرَّت عليها سنواتٌ من الاستخدام، لكنها تقوم بأمورٍ مُدمِّرة!

٢. التثبيت من قرص مضغوط

الخطوات الأساسية لتثبيت نسخة الخادوم من قرص مضغوط هي نفس الخطوات لتثبيت أي نظام تشغيل من قرص مضغوط؛ وعلى النقيض من نسخة سطح المكتب، لا تحتوي نسخة الخادوم على نظام تثبيت رسومي؛ حيث تَستخدِم نسخة الخادوم واجهةً نصيةً عوضًا عنها.

- بدايةً، نزِّل واحرق ملف ISO الملائم من موقع أوبنتو الرسمي.
- أقلع النظام من قارئة الأقراص المضغوطة.
- سيُطلَب منك تحديد اللغة في مِحَث الإقلاع (Boot prompt).

- هنالك بعض الخيارات الإضافية لتثبيت نسخة الخادوم من أوبنتو الموجودة في قائمة الإقلاع الرئيسية، يمكنك تثبيت خادوم أوبنتو أساسي، أو تفحص قرص CD-ROM والتأكد من خلوه من الأعطاب، أو التحقق من ذاكرة النظام (RAM)، أو الإقلاع من القرص الصلب الأول، أو إصلاح نظام معطوب؛ ستناقش بقية هذا القسم كيفية تثبيت خادوم أوبنتو أساسي.
- يسأل المثبت عن اللغة التي سيستخدمها، وبعد ذلك سيُطلَب منك أن تختار موقعك.
- الخطوة التالية هي سؤالك عن تحديد تخطيط لوحة المفاتيح الخاصة بك، يمكنك أن تطلب من المثبت أن يحاول أن يحددها لك، أو بإمكانك اختيارها يدويًا من القائمة.
- ثم سيكتشف المثبت إعدادات العتاد لديك، ثم سيحاول ضبط إعدادات الشبكة باستخدام DHCP، إذا لم تُرِد استخدام DHCP في الشاشة التالية، فاختر «رجوع»، حيث تستطيع الوصول إلى الخيار «هيئ الشبكة يدويًّا».
- سيُعَدّ مستخدمٌ جديد، وسيحصل هذا المستخدم على امتيازات الجذر باستخدام الأداة sudo.
- بعد إكمال إعدادات المستخدم، ستُسأل عمّا إذا أردت تشفير مجلد المنزل.
- سيسألك المثبت في الخطوة التالية عن اسم المضيف (hostname)، ومنطقة التوقيت.
- ثم بإمكانك الاختيار بين عدّة خيارات لضبط تخطيط القرص الصلب، بعد ذلك ستُسأل عن القرص الذي تريد تثبيت النظام عليه، ستحصل على نافذات للتأكيد قبل أن تعيد كتابة جدول الأقسام أو قبل إعداد LVM اعتمادًا على تخطيط القرص الصلب؛ إذا اخترت LVM، فستُسأل عن حجم القسم الجذر المنطقي؛ لخيارات الأقراص المتقدمة، راجع قسم «التثبيت المتقدم».
- سيُثبَّت بعد ذلك نظام أوبنتو الأساسي.

- الخطوة الآتية في عملية التثبيت هي تقرير كيفية تحديث النظام، حيث هناك ثلاثة خيارات:
  - بدون تحديثات تلقائية: وهذا ما يتطلب من المدير أن يسجل الدخول إلى الحاسوب ويثبت التحديثات يدويًا.
  - تثبيت التحديثات الأمنية تلقائيًا: وهذا ما سيثبت حزمة unattended-upgrades، التي ستُثبِّت التحديثات الأمنية دون تدخل من المدير؛ لمزيدٍ من المعلومات، راجع القسم «التحديثات التلقائية».
  - إدارة النظام باستخدام Lanscape: إن Lanscape هو خدمة مدفوعة من كانونيكال لتسهيل إدارة الأجهزة العاملة بنظام أوبنتو؛ راجع موقع Lanscape للتفاصيل.
- تملك الآن الخيار لتثبيت، أو عدم تثبيت، العديد من مجموعات الحزم؛ راجع القسم «مجموعات الحزم» لمزيد من التفاصيل. وهنالك أيضًا خيار لتشغيل aptitude لاختيار الحزم التي تريد تثبيتها، للمزيد من المعلومات، انظر القسم «الأداة Aptitude».
- في النهاية، آخر خطوة قبل إعادة الإقلاع هي ضبط الساعة على توقيت UTC (التوقيت العالمي).

ملاحظة: إذا لم تكن راضيًا عن الإعدادات الافتراضية في أيّة مرحلة من مراحل التثبيت، فاستخدم خاصية «رجوع» الظاهرة في أيّة نافذة لكي تذهب لقائمة التثبيت المفصلة، التي تسمح لك بتعديل الإعدادات الافتراضية.

ربما احتجت في نقطة ما أثناء عملية التثبيت إلى قراءة صفحة المساعدة التي يزودها نظام التثبيت، عندئذٍ اضغط على F1. مرةً أخرى، راجع «دليل تثبيت أوبنتو» للحصول على تعليمات تفصيلية.

ا. مجموعات الحزم

لديك خلال عملية تثبيت نسخة الخادوم خيارٌ لتثبيت حزم إضافية من القرص المضغوط، تُجَمَّع هذه الحزم بواسطة نوع الخدمة التي توفرها.

- خادوم DNS: تُحدِّد هذه المجموعة خادوم BIND DNS وتوثيقه.
- خادوم LAMP: تُحدِّد الحزم اللازمة لخادوم Linux-Apache-MySQL-PHP.
- خادوم Mail: هذه المجموعة تُحدِّد حزمًا متنوعة مفيدة لخادوم بريد ذي غرضٍ عام.
- خادوم OpenSSH: تحدد الحزم التي يحتاج خادوم OpenSSH لوجودها.
- قاعدة بيانات PostgreSQL: هذه المجموعة تحدد حزم العميل والخادوم لقواعد بيانات PostgreSQL.
- خادوم طباعة: تُهيِّء هذه المجموعة نظامك ليكون خادوم طباعة.
- خادوم ملفات سامبا: تُهيِّء هذه المجموعة نظامك ليكون خادوم ملفات سامبا (Samba File Server)، الذي يفيد خصوصًا في الشبكات التي فيها أنظمة ويندوز ولينُكس معًا.
- خادوم جافا «تومكات»: تُثبِّت هذه المجموعة خادوم «Apache Tomcat»، والاعتماديات اللازمة لعمله.
- مضيف آلات وهمية: تتضمن الحزم اللازمة لتشغيل آلات وهمية تعتمد على KVM.
- تحديد الحزم يدويًا: تنفيذ aptitude مما يسمح لك باختيار الحزم فرادى يدويًا.

تُثبَّت مجموعات الحزم باستخدام الأداة Tasksel، أحد أهم الفروقات بين أوبنتو (أو دبيان) وغيرها من توزيعات غنو/لينُكس هي أن الحزم عندما تُثبَّت فإنها تُضبَط ضبطًا منطقيًا، وتسألك في بعض الأحيان عن المعلومات الإضافية المطلوبة؛ وبشكل مشابه، عند تثبيت مجموعة حزم فإن الحزم لا تثبت فقط بل تُعَدّ أيضًا لتوفير خدمة مندمجة جيدًا مع بعضها بعضًا.

تستطيع مشاهدة قائمة بمجموعات الحزم المتوفرة بإدخال الأمر الآتي في مِحَث الطرفية بعد أن تنتهي عملية التثبيت:

```
tasksel --list-tasks
```

ملاحظة: سيُعرَض أيضًا في الناتج مجموعات الحزم من التوزيعات الأخرى المبينة على أوبنتو، مثل كوبنتو (Kubuntu)، وايديوبونتو (Edubuntu)، لاحظ أيضًا أنك تستطيع استدعاء الأمر tasksel لوحده، الذي سيعرض لك قائمةً بمختلف مجموعات الحزم المتوفرة.

تستطيع معرفة الحزم المثبتة مع أي مجموعة باستخدام الخيار task-packages--؛ على سبيل المثال، لعرض الحزم المثبتة مع مجموعة الحزم الخاصة بخادوم DNS، فإننا ندخل الأمر الآتي:

```
tasksel --task-packages dns-server
```

يجب أن يكون ناتج الأمر السابق:

```
bind9-doc
bind9utils
bind9
```

إذا لم تُثبَّت أيّة مجموعة حزم أثناء عملية التثبيت، لكنك مثلًا قررت أن تجعل خادوم LAMP الجديد عندك خادوم DNS أيضًا، فبإمكانك ببساطة إدراج قرص التثبيت وتنفيذ الأمر الآتي من الطرفية:

```
sudo tasksel install dns-server
```

٣. الترقية

هنالك عدة طرق للترقية من إصدارة أوبنتو لأخرى، سيعطيك هذا القسم لمحةً عن طريقة الترقية المستحسنة.

ا. الأداة do-release-upgrade

الطريقة المستحسنة لترقية نسخة الخادوم هي استخدام الأداة do-release-upgrade، التي هي جزءٌ من حزمة update-manager-core، وليس لديها أيّة اعتماديات رسومية، وهي مثبّتة تلقائيًا.

يمكن تحديث الأنظمة المبينة على دبيان باستخدام الأمر apt-get dist-upgrade، لكن استخدام الأداة do-release-upgrade مستحسن لأن بإمكان تلك الأداة التعامل مع التغيرات في ضبط النظام، الذي قد يكون لازمًا في بعض الأحيان بين الإصدارات.

اكتب الأمر الآتي في مِحَث الطرفية للترقية إلى إصدارة أحدث:

```
do-release-upgrade
```

من الممكن استخدم do-release-upgrade للترقية إلى إصدارة تطويرية من أوبنتو، أضف الخيار d- لفعل ذلك:

```
do-release-upgrade -d
```

تحذير: التحديث إلى إصدارة تطويرية هو أمر غير مستحسن في البيئات الإنتاجية.

٤. التثبيت المتقدم

أ. RAID برمجي

مصفوفة التعدد للأقراص المستقلة (Redundant Array of Independent Disks أو اختصارًا RAID) هي طريقة لاستخدام عدّة أقراص صلبة لتوفير توازن بين زيادة مرونة ووثوقيّة تخزين البيانات، و/أو زيادة أداء القراءة والكتابة، وذلك بالاعتماد على مستوى RAID المطبَّق؛ ويمكن تطبيق RAID إما بطريقة برمجية (حيث يَعلم نظام التشغيل عن القرصين المستخدمين، ويصون العلاقة بينهما)، أو عن طريق العتاد (حيث يضاف متحكم خاص يجعل نظام التشغيل يعتقد أنه يتعامل مع قرص واحد، ويتحكم بالأقراص تحكمًا «خفيًا»).

النسخة البرمجية من RAID الموجودة في الإصدارات الحالية من لينُكس (وأوبنتو) هي مبنية على محرك «mdadm» الذي يعمل عملًا ممتازًا، وحتى أنه أفضل من متحكمات RAID «الفيزيائية»؛ سيدلُّك هذا القسم على طريقة تثبيت نسخة الخادوم من أوبنتو باستخدام قسمَي RAID1 على قرصين صلبين منفصلين، واحد من أجل نظام ملفات الجذر (/)، والآخر لذاكرة التبديل(Swap).

التقسيم

اتّبِع تعليمات التثبيت إلى أن تصل إلى خطوة تقسيم الأقراص، عندها:

١. اختر طريقة التقسيم اليدوية.

٢. اختر القرص الصلب الأول، ووافق على «هل تريد إنشاء جدول تجزئة جديد وفارغ على هذا الجهاز؟»، أعد هذه الخطوة لجميع الأجهزة التي تريدها أن تصبح جزءًا من مصفوفة RAID.

٣. اختر «المساحة المتاحة» في أول قرص، ثم حدد «إنشاء جزء [قسم] جديد».

٤. اختر بعدها المساحة التخزينية لهذا القسم، سيكون هذا القسم هو القسم الخاص بذاكرة التبديل، والقاعدة العامة لحجم ذاكرة التبديل هي أن تكون ضعف حجم ذاكرة الوصول العشوائي (RAM)، اختر المساحة التخزينية للقسم، ثم اختر «أولي»، ثم «في البداية» (مكان بدء القطاعات).

ملاحظة: لا يُستحسَن دومًا أن يكون حجم ذاكرة التخزين ضعف حجم الذاكرة، وخصوصًا في الأنظمة التي تملك مقدارًا كبيرًا من الذاكرة، يتوقف حساب الحجم التخزيني لقسم ذاكرة التبديل على طريقة استخدام النظام.

٥. اختر سطر «طريقة الاستخدام» من الأعلى، الذي يكون افتراضيًا «نظام ملفات Ext4»، وغيرّه إلى «حجم فيزيائي لمصفوفة RAID» (أو «الكتلة الجسمية لـ RAID») ، ثم اختر «انتهى إعداد الجزء [القسم]».

٦. ولتهيئة قسم الجذر (/) فاختر «المساحة المتاحة» مرةً أخرى على القرص الصلب الأول، ثم اختر «إنشاء جزء [قسم] جديد».

٧. اختر ما تبقى من مساحة القرص التخزينية، ثم اضغط على متابعة، ثم «أولي».

٨. وكما في قرص ذاكرة التبديل، اختر «طريقة الاستخدام» ثم «حجم فيزيائي لمصفوفة RAID»، ثم اختر سطر «وسم إمكانية الإقلاع»، وغيرها إلى «ممكّن»، ثم اختر «انتهى إعداد الجزء [القسم]».

٩. أعد تنفيذ الخطوات من ثلاثة إلى ثمانية للأقراص والأقسام الأخرى.

إعداد RAID

بعد أن أُعِّدَت الأقسام، يمكن الآن ضبط المصفوفة:

١. عد إلى صفحة «تقسيم الأقراص» الرئيسية، واختر «تهيئة مصفوفة RAID البرمجية» بالأعلى.

٢. اختر «نعم» لكتابة التغيرات إلى القرص.

٣. اختر «إنشاء جهاز MD».

٤. لهذا المثال، اختر «RAID1»، لكن إن كنت تستخدم ضبطًا مختلفًا، فاختر النوع الملائم (RAID0، أو RAID1، أو RAID5).

ملاحظة: ستحتاج إلى ثلاثة أقراص على الأقل لاستخدام RAID5، أما استخدام RAID0 أو RAID1، فيلزمك قرصين فقط.

٥. أدخِل رقم الأجهزة الفعالة (٢)، أو مقدار الأقراص الصلبة التي عندك والتي ترغب باستخدامها في المصفوفة، ثم اختر «متابعة».

٦. أدخل رقم الأقراص البديلة (في حالة حدوث عطب في أحد الأقراص)، الذي هو «٠» افتراضيًا، ثم اختر «متابعة».

٧. اختر الأقسام التي تريد استخدامها، عمومًا، ستكون sda1, sdb1, sdc1 ...إلخ. ستتطابق الأرقام غالبًا، وستختلف الأحرف للدلالة على اختلاف الأقراص الصلبة.

٨. لقسم ذاكرة التبديل، اختر sda1، و sdb1، ثم اختر «متابعة» للذهاب للخطوة الآتية.

٩. أعد الخطوات من ثلاثة إلى سبعة لقسم الجذر (/) باختيار sda2، و sdb2.

١٠. بعد انتهائك من الضبط، اختر «إنهاء».

التهيئة

يجب أن تحصل الآن على قائمة بالأقراص الصلبة وأجهزة RAID، الخطوة الآتية هي التهيئة وإعداد نقاط الوصل لأجهزة RAID؛ عامل جهاز RAID كقرص صلب، هيِّئه وصِلْه كالمعتاد.

١. اختر «#1» تحت قسم «RAID1 برمجي الجهاز #0».

٢. اختر «استخدام ك»، ثم اختر «ذاكرة التبديل»، ثم «انتهى إعداد الجزء [القسم]».

٣. ثم اختر «#1» تحت قسم «RAID1 برمجي الجهاز #1».

٤. اختر «طريقة الاستخدام»، ثم اختر «نظام ملفات Ext4 سجلي».

٥. اختر «نقطة الوصل»، واضبطها على «/ - جذر نظام الملفات»، عدِّل الخيارات الأخرى كما تريد، ثم اختر «انتهى إعداد الجزء [القسم]».

٦. في النهاية، اختر «إنهاء التجزئة، وكتابة التغيرات إلى القرص».

إذا اخترت وضع قسم الجذر في مصفوفة RAID، فسيسألك المثبت إذا كنت تريد الإقلاع بحالة «منخفضة» (degraded)، راجع القسم «مصفوفة RAID ذات الحالة المتدهورة (degraded state)» للمزيد من التفاصيل. يجب أن تُكمَل عملية التثبيت بشكلٍ اعتيادي.

مصفوفة RAID ذات الحالة المتدهورة (degraded state)

قد يحصل خلل في القرص في نقطة ما من حياة الحاسوب؛ وعندما يحصل ذلك وقت استخدام مصفوفة RAID برمجية، فسيضع نظام التشغيل المصفوفة في ما يدعى «الحالة المتدهورة» (degraded state).

إذا أصبحت المصفوفة في الحالة المتدهورة -ربما لحدوث تلف في البيانات- فعندها تحاول نسخة الخادوم من أوبنتو افتراضيًا الإقلاع إلى initramfs بعد ثلاثين ثانية، وعندما يكتمل إقلاع initramfs، فسيظهر مِحَث لمدة خمس عشرة ثانية يسمح لك بالاختيار بين إقلاع النظام أو محاولة استرداده يدويًا؛ ربما لا يكون الإقلاع إلى محث initramfs هو السلوك المطلوب، وخصوصًا إن كان الحاسوب في مكان بعيد عنك. يمكن إعداد الإقلاع إلى مصفوفة متدهورة بعدة طرق:

- الأداة dpkg-reconfigure التي تستخدم لضبط السلوك الافتراضي؛ وسُتسأل خلال العملية عن الخيارات الإضافية المتعلقة بالمصفوفة، كالمراقبة، وتنبيهات البريد ...إلخ. أدخِل الأمر الآتي لإعداد mdadm:

```
sudo dpkg-reconfigure mdadm
```

- ستغير عملية dpkg-reconfigure mdadm ملف الإعدادات /etc/initramfs-tools/conf.d/mdadm، لدى هذا الملف ميزة القدرة على الإعداد المسبق لسلوك النظام، ويمكن تعديله يدويًا:

```
BOOT_DEGRADED=ture
```

ملاحظة: يمكن تجاوز ملف الإعدادات باستخدام وسيط يمرر للنواة.

يَسمح استخدام وسيط يمرر للنواة لك أيضًا بإقلاع النظام من مصفوفة ذات الحالة المتدهورة كما يلي:

- عندما يقلع الخادوم، اضغط على Shift لفتح قائمة جروب (Grub).
- اضغط e لتعديل خيارات النواة.
- اضغط على زر السم السفلي لتعليم سطر النواة.
- أضف «bootdegraded=true» (دون علامات الاقتباس) إلى نهاية السطر.
- اضغط على Ctrl+x لإقلاع النظام.

بعد أن يُقلِع النظام، تستطيع إما إصلاح المصفوفة (انظر قسم «صيانة مصفوفات RAID» للتفاصيل) أو نسخ المعلومات المهمة إلى جهاز آخر بسبب عطب في العتاد.

صيانة مصفوفات RAID

يمكن أن تَعرِض الأداة mdadm حالة المصفوفة، أو تستطيع إضافة أو إزالة أقراص في المصفوفة ...إلخ.

- لإظهار حالة مصفوفة أقراص، فأدخِل الأمر الآتي إلى الطرفية:

```
sudo mdadm -D /dev/md0
```

الخيار D- يخبر mdadm أن يُظهِر معلوماتٍ تفصيلية حول الجهاز dev/md0/، استبدل مسار جهاز RAID المناسب بالمسار dev/md0/.

- لعرض حالة قرص في مصفوفة:

```
sudo mdadm -E /dev/sda1
```

ستُشابِه مخرجات الأمر السابق مخرجات الأمر mdadm -D؛ عدِّل /dev/sda1 لكل قرص من أقراص المصفوفة.

- إذا عُطِبَ قرصٌ ما، فيجب أن يُزال من المصفوفة:

```
sudo mdadm --remove /dev/mo0 /dev/sda1
```

بدِّل كلًّا من /dev/md0 و /dev/sda1 إلى جهاز RAID والقرص الملائمَين بالتوالي وبالترتيب.

- وبطريقة مشابهة، لإضافة قرص جديد:

```
sudo mdadm --add /dev/md0 /dev/sda1
```

يمكن أن تُبَدَّل حالة القرص في بعض الأحيان إلى «مُعَاب» (faulty)، حتى وإن لم يكن فيه خلل فيزيائي؛ من المفيد في كثير من الأحيان إزالة القرص من المصفوفة، ثم إعادة إضافته؛ وهذا ما يجعل القرص يُزامَن مرةً أخرى مع المصفوفة؛ وإذا لم يزامن القرص مع المصفوفة، فهذا دليلٌ قويٌ على وجود مشكلة فيزيائية فيه.

يحتوي الملف /proc/mdstat على معلومات مفيدة حول حالة أجهزة RAID في النظام:

```
cat /proc/mdstat
Personalities : [linear] [multipath] [raid0] [raid1] [raid6]
[raid5] [raid4] [raid10]
md0 : active raid1 sda1[0] sdb1[1]
      10016384 blocks [2/2] [UU]
unused devices: <none>
```

الأمر الآتي رائع لمشاهدة حالة مزامنة قرص:

```
watch -n1 cat /proc/mdstat
```

اضغط على Ctrl+c لإيقاف الأمر watch.

إذا احتجت لاستبدال قرص معطوب، فيجب أن يعاد تثبيت محمل الإقلاع «جروب» (grub) مرةً أخرى بعد استبدال القرص المعطوب بالجديد ومزامنته؛ أدخِل الأمر الآتي لتثبيت «جروب» على القرص الجديد:

```
sudo grub-install /dev/md0
```

ضع اسم جهاز المصفوفة الملائم بدلًا من /dev/md0.

ب. مصادر

إن موضوع مصفوفات RAID هو موضوع معقد نتيجةً لوفرة الطرق التي يمكن ضبط RAID فيها، رجاءً راجع الروابط الآتية لمزيدٍ من المعلومات:

- المقالات التي تتحدث عن «RAID» في ويكي أوبنتو.
- مقالة بعنوان «Software RAID HOWTO».
- كتاب «Managing RAID on Linux».

ج. مدير الحجوم المنطقية LVM

يسمح مدير الحجوم المنطقية (Logical Volume Manager) لمدراء الأنظمة بإنشاء حجوم تخزينية على قرصٍ واحد أو أقراصٍ صلبة متعددة؛ ويمكن إنشاء حجوم LVM على أقسام في مصفوفة RAID أو على الأقسام الموجودة في قرص واحد، ويمكن أيضًا توسيع تلك الحجوم، مما يضيف مرونةً كبيرةً للنظام عندما تتغير المتطلبات التشغيلية.

لمحة عامة

تأثيرٌ جانبي لقوة ومرونة LVM هو درجة كبيرةٌ من التعقيد؛ ويجدر بنا التعرف على بعض المصطلحات قبل الخوض في عملية تثبيت LVM:

- **الحجم الفيزيائي (PV):** القرص الصلب الفيزيائي، أو قسم في قرص، أو قسم مصفوفة RAID برمجية؛ مهيئين للعمل كحجم LVM.
- **مجموعة الحجوم (VG):** التي تُصنَع من حجم فيزيائي واحد أو أكثر؛ ويمكن أن تُوسَّع مجموعة الحجوم بإضافة المزيد من الحجوم الفيزيائية، حيث تكون مجموعة الحجوم كقرص صلب وهمي (virtual disk drive)، الذي يُنشَأ منه المزيد من الحجوم المنطقية.
- **حجم منطقي (LV):** الذي يشبه القسم في الأنظمة الأخرى (التي ليست LVM)، حيث يُهيّأ الحجم المنطقي بنظام الملفات المطلوب (Ext3، أو XFS، أوJFS ...إلخ.)، ويكون متوفرًا للوصل وتخزين البيانات.

التثبيت

سيشرح المثال في هذا القسم طريقة تثبيت نسخة الخادوم من أوبنتو مع وصل مجلد srv/ على حجم LVM، إذ سيُضاف حجمٌ فيزيائيٌ (PV) واحدٌ فقط أثناء عملية التثبيت، والذي يمثِّل جزءًا من مجموعة الحجوم؛ وسيضاف حجم فيزيائي آخر بعد التثبيت لشرح كيف يمكن أن تُوسَّع مجموعة الحجوم.

هنالك خياراتُ تثبيتٍ عدّة لاستخدام LVM، الخيار الأول «موجّه - استخدام القرص بأكمله وإعداد LVM» الذي يسمح بإعطاء جزء من المساحة التخزينية المتوفرة لاستخدامها في LVM، والخيار الآخر «موجّه - استخدام القرص بأكمله وإعداد LVM مشفّر»، أو إعداد الأقسام وضبط LVM يدويًا؛ والطريقة الوحيدة لهذه اللحظة لإعداد النظام لاستخدام LVM والأقسام الاعتيادية أثناء التثبيت هو استخدام الطريقة اليدوية.

١. اتَّبِع خطوات التثبيت إلى أن تصل إلى خطوة «تقسيم الأقراص»، عندها:
٢. في صفحة «تقسيم الأقراص»، اختر «يدويًا».
٣. اختر القرص الصلب، ثم في الشاشة التالية اختر «نعم» للرد على الرسالة «هل تريد إنشاء جدول تجزئة جديد وفارغ على هذا الجهاز؟».
٤. ثم أنشئ أقسام boot/، و swap، و / بأي نظام ملفات تريد.
٥. ولإنشاء srv/ باستخدام LVM، فأنشئ قسمًا منطقيًا جديدًا، ثم غير «طريقة الاستخدام» إلى «حجم فيزيائي لتخزين LVM»، ثم اختر «انتهى إعداد الجزء [القسم]».
٦. اختر الآن «إعداد مدير الحجوم المنطقية» في الأعلى، ثم اختر «نعم» لكتابة التعديلات إلى القرص.

٧. والآن اختر «إنشاء مجموعة حجوم» في «إعدادات LVM» في الشاشة التالية، ثم اختر اسمًا لمجموعة الحجوم، وليكن vg01، أو أي شيء يصفها أكثر من ذلك؛ وبعد اختيار الاسم، اختر القسم المُعَدّ لاستخدام LVM عليه، ثم «متابعة».

٨. وبالعودة لصفحة «إعدادات LVM»، اختر «إنشاء حجم منطقي»، واختر مجموعة الحجوم المُنشَأة منذ قليل، وأدخل اسمًا للحجم المنطقي الجديد (على سبيل المثال srv لأنه اسم نقطة الوصل المخطط لها) ثم اختر المساحة التخزينية، التي ستكون القسم بأكمله، لا تنسَ أنه يمكنك دائمًا زيادتها لاحقًا، ثم اختر «إنهاء» ويجب أن تعود لشاشة «تقسيم الأقراص».

٩. لإضافة نظام ملفات إلى LVM الجديد، اختر القسم تحت «LVM VG vg01, LV srv»، أو أي اسم قد اخترته في الخطوة السابقة، ثم اختر «طريقة الاستخدام»، واضبط نظام الملفات كالمعتاد باختيار srv/ نقطةً للوصل، ثم اضغط على «انتهى إعداد الجزء [القسم]» عند الفراغ منه.

١٠. في النهاية، اختر «إنهاء التجزئة وكتابة التغيرات إلى القرص»، ثم وافق على إجراء التغيرات، وأكمل عملية التثبيت.

هذه بعض الأدوات المفيدة لعرض المعلومات حول LVM:

- الأمر pvdisplay: عرض معلومات حول الحجوم الفيزيائية.
- الأمر vgdisplay: عرض معلومات حول مجموعات الحجوم.
- الأمر lvdisplay: عرض معلومات حول الحجوم المنطقية.

توسيع مجموعات الحجوم

بإكمال مثالنا المتعلق بحجم LVM واستخدامه كنقطة وصل لمجلد srv/، فسيناقش هذا القسم إضافة قرص صلب آخر، وإنشاء حجم فيزيائي (PV)، وإضافته إلى مجموعة الحجوم (VG)، وتوسيع الحجم المنطقي srv، ثم في النهاية توسيع نظام الملفات؛ يفترض هذا المثال أنَّ قرصًا صلبًا ثانيًا قد أُضيف إلى النظام، وفي هذا المثال، سيكون اسمه dev/sdb/ وسنستخدم القرص بأكمله كحجمٍ فيزيائي (بإمكانك إنشاء أقسام واستخدامها كحجوم فيزيائية مختلفة).

تحذير: تأكد أنه ليس لديك قرص صلب باسم dev/sdb/قبل تنفيذ الأوامر الآتية، قد تخسر بعض البيانات إذا نفَّذت هذه الأوامر على قرص غير فارغ.

أولًا، أنشِئ الحجم الفيزيائي بتنفيذ الأمر الآتي في الطرفية:

```
sudo pvcreate /dev/sdb
```

وسِّع الآن مجموعة الحجوم (VG):

```
sudo vgextend vg01 /dev/sdb
```

استخدم vgdisplay لمعرفة الامتدادات الفيزيائية أو PE (physical extents)، التي هي الامتدادات الفيزيائية الحرة / الحجم (الحجم التخزيني الذي حددته)، سنعتبر أن المساحة الفارغة هي ٥١١ PE (مما يساوي ٢ غيغابايت إذا كان حجم PE هو ٤ ميغابايت)، وسنستخدم كل المساحة الفارغة المتاحة، لا تنسَ استخدام رقم PE -أو الحجم التخزيني الحر- المتوفر عندك.

يمكن توسيع الحجم المنطقي بعدّة طرق، وسنشرح كيفية استخدام PE لتوسعة حجم منطقي:

```
sudo lvextend /dev/vg01/srv -l +511
```

إن الخيار l- يسمح بتوسعة الحجم المنطقي باستخدام PE، يسمح الخيار L- للحجم المنطقي بأن يُوسَّع باستخدام الميغا، أو الغيغا، أو التيرابايت ...إلخ.

حتى وإن كان من المفترض أنه باستطاعتك توسيع نظام ملفات ext3 أو ext4 دون فصله أولًا، لكن من العادات الجيدة فصله على أيّة حال وتفحص نظام الملفات؛ وبهذا لن تخرِّب شيئًا في اليوم الذي تريد فيه تقليل الحجم المنطقي (إذ يكون فصل نظام الملفات في هذه الحالة إلزاميًا).

الأوامر الآتية لأنظمة الملفات EXT3 أو EXT4، إذا كنت تستخدم أنظمة ملفات أخرى، فتتوفر أدوات مختلفة:

```
sudo umount /srv
sudo e2fsck -f /dev/vg01/srv
```

الخيار f- يجبر الأداة e2fsck على تفحص نظام الملفات وإن كان يبدو «نظيفًا».

في النهاية، غيِّر حجم نظام الملفات:

```
sudo resize2fs /dev/vg01/srv
```

ثم صِل نظام الملفات وتأكد من حجمه التخزيني:

```
mount /dev/vg01/srv /srv && df -h /srv
```

د. مصادر

- راجع المقالات حول LVM في ويكي أوبنتو.
- انظر مقالة LVM HOWTO للمزيد من المعلومات.
- مقالة أخرى جيدة هي «Managing Disk Space with LVM» في موقع O'Reilly المدعو LinuxDevCenter.com.
- للمزيد من المعلومات حول fdisk، انظر صفحة الدليل الخاصة به.

٥. تفريغ انهيار النواة

ا. مقدمة

يشير تفريغ انهيار النواة (Kernel Crash Dump) إلى جزء من محتويات ذاكرة الوصول العشوائي غير الدائمة التي تُنسَخ إلى القرص عندما يتعرض تنفيذ النواة إلى اضطراب ما، الأحداث الآتية تسبب اضطراب النواة:

- ارتياع النواة (Kernel Panic).
- تقطعات غير مقنَّعة (Non Maskable Interrupts [NMI]).
- استثناءات تفحص الجهاز (Machine Check Exceptions [MCE]).
- عطب في العتاد.
- تدخل يدوي.

لبعض تلك الأحداث (الارتياع، أو NMI)، سيكون رد فعل النواة تلقائيًا، وتُطلَق آلية تفريغ انهيار النواة عبر kexec، يلزم التدخلُ اليدوي في الحالات الأخرى للحصول على معلومات الذاكرة، وعندما تقع إحدى الأحداث السابقة، فيجب معرفة السبب الرئيسي للتمكن من تجنبه مستقبلًا؛ يمكن تحديد السبب بتفحص محتويات الذاكرة المنسوخة.

ب. آلية تفريغ انهيار النواة

عندما يحدث ارتياع النواة، فإن النواة تعتمد على آلية kexec لتعيد الإقلاع بسرعة لنسخةٍ جديدةٍ من النواة في القسم المحفوظ من الذاكرة المحجوزة عندما أقلع النظام (انظر في الأسفل)، وهذا يسمح لمنطقة الذاكرة المتبقية أن تبقى دون أن تُلمَس لنسخها نسخًا آمنًا إلى وسيطة التخزين.

ج. التثبيت

تُثبَّت أداة تفريغ انهيار النواة بالأمر الآتي:

```
sudo apt-get install linux-crashdump
```

د. الضبط

عدِّل الملف /etc/default/kdump-tool مضيفًا السطر الآتي:

```
USER_KDUMP=1
```

يجب إعادة إقلاع النظام بعد ذلك.

٥. التحقق

للتأكد من أن آلية تفريغ انهيار النواة مفعَّلة، فهنالك عدّة أمور يجب التحقق منها، تأكد أولًا من أن مُعامِل الإقلاع crashkernel موجودٌ (لاحظ أن الأسطر الآتية قد قُسِّمَت لكي تظهر في الكتاب بشكل سليم):

```
cat /proc/cmdline
BOOT_IMAGE=/vmlinuz-3.2.0-17-server root=/dev/mapper/PreciseS-
↪ root ro crashkernel=384M-2G:64M,2G-:128M
```

لمعامل crashkernel الشكل العام الآتي:

```
crashkernel=<range1>:<size1>[,<range2>:<size2>,...][@offset]
↪ range=start-[end] 'start' is inclusive and 'end' is exclusive.
```

لذا، لمعامل crashkernel الذي وجدناه في ملف /proc/cmdline، سيكون لدينا:

```
crashkernel=384M-2G:64M,2G-:128M
```

السطر السابق يعني الآتي:

- إذا كانت قيمة الذاكرة في النظام أقل من ٣٨٤ ميغابايت، فلا تُبقي على شيء (هذه هي حالة «الإنقاذ» [rescue]).
- إذا كانت قيمة الذاكرة في النظام بين ٣٨٤ ميغابايت و ٢ غيغابايت (بما فيها ٢ غيغابايت)، فحافظ على ٦٤ ميغابايت.
- إذا كان حجم الذاكرة في النظام أكبر من ٢ غيغابايت، فحافظ عندها على ١٢٨ ميغابايت.

ثانيًا، يجب التأكد من أن النواة قد حافظت على مكان الذاكرة المطلوبة للأداة kdump باستخدام:

```
dmesg | grep -i crash
...
[ 0.000000] Reserving 64MB of memory at 800MB for crashkernel
(System RAM: 1023MB)
```

و. اختبار آلية تفريغ انهيار النواة

تحذير: سيؤدي اختبار آلية تفريغ انهيار النواة إلى إعادة إقلاع النظام، وقد يسبب ذلك فقدانًا للبيانات في بعض الأحيان إذا كان النظام تحت حِملٍ شديد؛ إذا أردت اختبار الآلية فتأكد من أن نظامك لا يجري أيّة عمليات مهمة، أو أنَّه تحت حمل خفيف جدًا.

تأكد من أن آلية SysRq مُفعَّلة بالنظر إلى قيمة معامل النواة في /pro/sys/kernel/sysrq:

```
cat /proc/sys/kernel/sysrq
```

إذا أُعيدَت القيمة "صفر"، فإن تلك الميزة معطلة، وعليك تنفيذ الأمر الآتي لتفعيلها:

```
sudo sysctl -w kernel.sysrq=1
```

بعد فعل ذلك، يجب أن تصبح المستخدم الجذر حيث لا يكفي استخدام sudo؛ وعليك كمستخدم جذر تنفيذ الأمر:

```
echo c > /proc/sysrq-trigger
```

وإذا كنت تستخدم اتصالًا شبكيًا، فستفقد تواصلك مع النظام ولهذا من الأفضل أن تختبر ذلك عندما تكون موصولًا للنظام عبر طرفية محلية، مما يجعل عملية تفريغ النواة ظاهرةً أمامك.

إن ناتج فحصٍ عادي سيكون شبيهًا بما يلي:

```
sudo -s
[sudo] password for ubuntu:
# echo c > /proc/sysrq-trigger
[ 31.659002] SysRq : Trigger a crash
[ 31.659749] BUG: unable to handle kernel NULL pointer
dereference at       (null)
[ 31.662668] IP: [<ffffffff8139f166>]
sysrq_handle_crash+0x16/0x20
[ 31.662668] PGD 3bfb9067 PUD 368a7067 PMD 0
[ 31.662668] Oops: 0002 [#1] SMP
[ 31.662668] CPU 1
....
```

لقد أُقتطِعَت بقية السجل، لكن يجب أن تشاهد أن النظام قد أعيد إقلاعه في مكان ما في السجل، حيث سترى السطر الآتي:

```
Begin: Saving vmcore from kernel crash ...
```

عند الإكمال، سيُعاد تشغيل النظام لحالته الاعتيادية، وستجد ملف تفريغ انهيار النواة في مجلد /var/crash:

```
ls /var/crash
linux-image-3.0.0-12-server.0.crash
```

ز. مصادر

تفريغ انهيار النواة هو موضوع واسع يتحاج إلى خبرات في نواة لينُكس، تستطيع إيجاد المزيد من المعلومات حول الموضوع في:

- توثيق kdump.
- الأداة crash.
- مقالة «تحليل تفريغ انهيار نواة لينُكس» (هذه المقالة مبنية على فيدورا، لكنها تشرح تحليل تفريغ النواة جيدًا).

٣

إدارة الحزم

توفر أوبنتو نظام إدارةَ حزمٍ شاملٍ للتثبيت والترقية والضبط وإزالة البرمجيات، بالإضافة إلى توفير الوصول إلى أكثر من ٣٥٠٠٠ حزمة برمجيات منظَّمة؛ وأيضًا من ميزات نظام إدارة الحزم حل مشاكل الاعتماديات، والتحقق من وجود تحديثات للبرمجيات.

هنالك عدة أدوات متوفرة للتعامل مع نظام إدارة الحزم الخاص بأوبنتو، بدءًا من الأدوات البسيطة التي تعمل من سطر الأوامر، التي يمكن بسهولةٍ أتمتةُ عملها من مدراء النظام، ووصولًا إلى واجهة رسومية بسيطة تكون سهلةً على الوافدين الجدد لنظام أوبنتو.

١. مقدمة

أُشتُق نظام إدارة الحزم في أوبنتو من نفس النظام المستخدم في توزيعة دبيان غنو/لينُكس. تحتوي ملفات الحزم على جميع الملفات اللازمة، والبيانات الوصفية، والتعليمات لتشغيل وظيفة معينة أو برنامج محدد على حاسوبك العامل بنظام تشغيل أوبنتو.

تكون لملفات حزم دبيان عادةً اللاحقة «.deb»، وتتواجد غالبًا في مستودعات (repositories)، التي هي مجموعات من الحزم الموجودة في وسائط مختلفة، كأقراص CD-ROM، أو على الإنترنت؛ تلك الحزم مُصرَّفة (compiled) مسبقًا إلى صيغة ثنائية في غالب الأحيان، لذلك يكون تثبيتها سريعًا، وبالتالي لا تحتاج لبناء البرمجية من المصدر.

تَستخدم حزمٌ عديدةٌ معقدةٌ المصطلحَ «الاعتماديات» (dependencies)؛ الاعتماديات هي الحزم الإضافية التي تتطلبها حزمة رئيسية لأداة الوظيفة المطلوبة أداءً سليمًا؛ على سبيل المثال، حزمة تركيب الكلام المسماة festival تعتمد على حزمة libasound2، التي توفر مكتبة الصوت ALSA الضرورية لتشغيل الصوت، ولكي يعمل festival عملًا صحيحًا، يجب أن يُثبَّت هو وجميع اعتمادياته؛ حيث تُجري أدوات إدارة البرمجيات في أوبنتو ذلك تلقائيًا.

٢. الأداة dpkg

dpkg هو مدير حزم للأنظمة المبينة على دبيان؛ حيث يمكنه تثبيت، وحذف، وبناء الحزم، ولكن على النقيض من بقية أنظمة إدارة الحزم، لا يمكنه أن يُنزِّل ويُثبِّت الحزم أو اعتمادياتها تلقائيًا؛ سيغطي هذا القسم استخدام dpkg لإدارة الحزم المثبتة محليًا:

اكتب الأمر الآتي في الطرفية لعرض كل الحزم المثبتة على النظام:

```
dpkg -l
```

وبالاعتماد على عدد الحزم المثبتة على نظامك، يمكن أن يُولِّد الأمر السابق ناتجًا ضخمًا من البيانات؛ تستطيع تمرير الناتج عبر أنبوب للأداة grep لمعرفة فيما إذا كانت حزمة معينة قد ثُبِّتَت على النظام:

```
dpkg -l | grep apache2
```

استبدل اسم الحزم التي تريد البحث عنها، أو جزءًا منه، أو تعبيرًا نمطيًا (regular expression)، باسم الحزمة apache2.

لعرض الملفات المثبتة بواسطة حزمة ما، في هذه الحالة حزمة ufw، فأدخِل الأمر:

```
dpkg -L ufw
```

إذا لم تكن متأكدًا أيّة حزمة قد ثبتت ملفًا ما، فالأمر dpkg -S سيخبرك، على سبيل المثال:

```
dpkg -S /etc/host.conf
base-files: /etc/host.conf
```

تُظهِر المخرجات أنَّ الملف /etc/host.conf ينتمي إلى الحزمة base-files.

ملاحظة: العديد من الملفات تولَّد تلقائيًا أثناء عملية تثبيت الحزمة، وعلى الرغم من أن تلك الملفات موجودة في نظام الملفات، فقد لا يعلم dpkg -S أيّة حزمة تنتمي إليها تلك الملفات.

بإمكانك تثبيت ملف حزمة deb. بالأمر الآتي:

```
sudo dpkg -i zip_3.0-4_i386.deb
```

ضع اسم ملف الحزمة التي تريد تثبيتها عندك بدلًا من zip_3.0-4_i386.deb.

يمكن إلغاء تثبيت حزمة معينة بالأمر:

```
sudo dpkg -r zip
```

تحذير: ليس من المستحسن في معظم الحالات إلغاء تثبيت الحزم باستخدام dpkg، من الأفضل استخدام مدير حزم يستطيع حل مشاكل الاعتماديات للتأكد من أن النظام في حالة «متينة»، فعلى سبيل المثال، استخدام dpkg -r zip سيحذف حزمة zip، لكن أيّة حزم تعتمد عليها ستبقى مثبتةً ولكنها لن تعمل بصورة صحيحة.

للمزيد من خيارات dpkg، راجع صفحة الدليل man dpkg.

٣. الأداة Apt-Get

إن الأداة apt-get هي أداة سطر أوامر مفيدة جدًا، إذ تتعامل مع «أداة التحزيم المتقدمة» (Advanced Packaging Tool ‏[APT])، وتُنفِّذ مهامًا كتثبيت حزم البرمجيات الجديدة، وترقية الحزم البرمجية الموجودة، وتحديث فهرس قائمة الحزم، وحتى ترقية كامل نظام أوبنتو.

كون هذه الأداة أداةً سطرية (أي تعمل من سطر الأوامر)، فإن للأداة apt-get مزايا كثيرةً تتميز بها عن غيرها من أدوات إدارة الحزم المتوفرة في أوبنتو لمدراء الخواديم، إحدى تلك المزايا هي سهولة الاستخدام في جلسات الطرفية البسيطة (عبر SSH)، وقابلية الاستخدام في سكربتات إدارة الأنظمة، التي يمكن أن تؤتمت باستخدام أداة جدولة المهام cron.

بعض الأمثلة للاستخدامات الشائعة للأداة apt-get:

تثبيت حزمة: عملية تثبيت الحزم باستخدام أداة apt-get هي عمليةٌ سهلةٌ جدًا؛ فعلى سبيل المثال، اكتب الأمر الآتي لتثبيت حزمة ماسح الشبكة nmap:

```
sudo apt-get install nmap
```

حذف حزمة: أيضًا عملية حذف حزمة (أو حزم) هي عملية مباشرة جدًا؛ فلحذف الحزمة التي ثبتناها في المثال السابق، فإننا نستخدم الأمر الآتي:

```
sudo apt-get remove nmap
```

تلميح: يمكنك تحديد أكثر من حزمة لتثبِّت أو تحذف، وذلك بتمرير أسماء تلك الحزم كوسائط للأمر apt-get مفصولةً بفراغات.

إن إضافة الخيار --purge إلى الأمر apt-get remove سيجعل apt-get يحذف ملفات إعدادات الحزمة أيضًا، ربما يكون -أو لا يكون- هذا ما تريده؛ استخدم هذا الخيار بعد أخذ الحيطة والحذر.

تحديث فهرس قائمة الحزم: إن فهرس حزم APT هو قاعدة بيانات للحزم المتوفرة في المستودعات المعرَّفة في ملف /etc/apt/sources.list وفي مجلد /etc/apt/sources.list.d؛ فلتحديث فهرس الحزم المحلي والحصول على آخر التعديلات التي أُجريَت على المستودعات، فعليك تنفيذ الأمر الآتي:

```
sudo apt-get update
```

لمعلومات حول كيفية الترقية إلى إصدارة جديدة من أوبنتو، ألقِ نظرةً على قسم «الترقية».

العمليات التي أجريت بواسطة الأداة apt-get، كتثبيت وحذف الحزم، ستُسجَّل في ملف السجل /var/log/dpkg.log.

للمزيد من المعلومات حول استخدام APT، راجع «دليل مستخدم APT في دبيان»، أو اكتب:

```
apt-get help
```

٤. الأداة Aptitude

سيعطيك تشغيل Aptitude دون خيارات سطر الأوامر واجهةً نصيةً لنظام التحزيم المتقدم (APT)، العديد من وظائف إدارة الحزم الشائعة، كالتثبيت، والحذف، والترقية يمكن إجراؤها في Aptitude بأمرٍ ذي حرفٍ واحد، الذي يكون عادةً بأحرفٍ ذاتُ حالةٍ صغيرة.

يعمل Aptitude جيدًا في البيئات النصية التي تكون طرفياتٍ دون واجهة رسومية، لعدم حدوث تضارب في أزرار الأوامر؛ يمكنك بدء واجهة ذات قوائم من Aptitude بكتابة الأمر الآتي في مِحَث الطرفية:

```
sudo aptitude
```

ستشاهد شريط القائمة في أعلى الشاشة عندما يبدأ Aptitude، وجزأين تحته، يحتوي الجزء العلوي على تصنيفات الحزم، كالحزم الجديدة، والحزم غير المثبتة؛ وأما الجزء السفلي فيحتوي على معلومات تتعلق بالحزم وتصنيفاتها.

عملية استخدام Aptitude لإدارة الحزم هي عملية مباشرة إلى حدٍ ما؛ وتجعلُ واجهةُ المستخدمِ من المهام الشائعة أمرًا هينًا ليقام به؛ ما يلي أمثلةٌ عن كيفية تنفيذ وظائف إدارة الحزم الأساسية في Aptitude:

- تثبيت الحزم: لتثبيت حزمة ما، حدِّد الحزمة في تصنيف «الحزم غير المثبتة»، وذلك باستخدام أزرار الأسهم في الحاسوب وزر Enter، علِّم على الحزم المُراد تثبيتها ثم اضغط على زر +، حيث سيتبدَّل لون مدخلة الحزمة إلى اللون الأخضر، مما يشير إلى أنها قد حُدِّدَت للتثبيت؛ اضغط الآن على الزر g لإظهار ملخص عن الأفعال التي ستُجرى

على الحزم، اضغط على g مرةً أخرى، وسيُطلَب منك أن تصبح جذرًا لإكمال التثبيت، اضغط على Enter، وسيُطلَب منك إدخال كلمة المرور، أدخل كلمة المرور لتصبح جذرًا؛ في النهاية، اضغط على g مرةً أخرى، فستُسأل عن تنزيل تلك الحزمة اضغط على Enter للمتابعة، ثم ستُجرى عملية تنزيل وتثبيت الحزمة.

- حذف الحزم: لحذف حزمة ما، حدد الحزمة في تصنيف «الحزم المثبتة»، وذلك باستخدام أزرار الأسهم في الحاسوب وزر Enter، علّم على الحزم المُراد حذفها ثم اضغط على زر "-"، حيث سيتبدَّل لون مدخلة الحزمة إلى اللون الوردي، مما يشير إلى أنها قد حُدِّدَت للحذف؛ اضغط الآن على الزر g لإظهار ملخص عن الأفعال التي ستُجرى على الحزم، اضغط على g مرةً أخرى، وسيطلب منك أن تصبح جذرًا لإكمال التثبيت، اضغط على Enter، وسيُطلب منك إدخال كلمة المرور، أدخل كلمة المرور لتصبح جذرًا؛ في النهاية، اضغط على g مرةً أخرى، واضغط على Enter للمتابعة، ثم ستُجرى عملية إزالة الحزمة.
- تحديث فهرس الحزم: لتحديث فهرس الحزم، اضغط ببساطة على الزر u، وستُسأل عمّا إذا كنت تريد أن تصبح جذرًا وتكمل التحديث، اضغط على Enter، وستُطالب بكلمة المرور، أدخل كلمة المرور لتصبح جذرًا، وسيبدأ تحديث فهرس الحزم؛ اضغط على Enter على زر OK في مربع الحوار الذي سيظهر عندما تنتهي عملية التنزيل.
- ترقية الحزم: لترقية الحزم، عليك أولًا تحديث فهرس الحزم كما وضِّح سابقًا، ثم اضغط على الحرف U لتحديد جميع الحزم التي لها تحديثات، اضغط الآن على الزر g حيث سيُعرَض لك ملخص عن الأفعال التي ستُجرى على الحزم، اضغط على g مرة أخرى، وسيُطلب منك أن تصبح جذرًا لإكمال التثبيت، اضغط على Enter، وستُطالب بكلمة المرور، أدخل كلمة مرور الجذر ثم اضغط على g مرة أخرى، وستُسأل عن تنزيل الحزم، اضغط على Enter للإكمال، وستبدأ عملية ترقية الحزم.

العمود الأول من المعلومات الظاهر في الجزء العلوي في قائمة الحزم يعرض حالة الحزمة، المفاتيح الآتية تصف حالة الحزمة:

- i: الحزمة مثبتة.
- c: الحزمة غير مثبتة، لكن إعدادات الحزمة ما زالت باقيةً على النظام.
- p: حذفت الحزمة حذفًا كاملًا من النظام (هي وإعداداتها).
- v: حزمة ظاهرية (Virtual package).
- B: حزمة محطمة (Broken package).
- u: ملفات الحزمة قد فُكَّ ضغطها، لكن الحزمة لم تُعَدّ بعد.
- C: الحزمة نصف مضبوطة، أي أن الضبط قد فشل، ويلزمه إصلاح.
- H: الحزمة نصف مثبتة، فشل الحذف، ويلزمه إصلاح.

للخروج من Aptitude، اضغط على حرف q، ووافق أنك تريد الخروج؛ يمكن الوصول لوظائف عديدة من وظائف Aptitude بالضغط على زر F10.

ا. استخدام Aptitude في سطر الأوامر

يمكنك استخدام Aptitude كأداةٍ سطرية (تعمل من سطر الأوامر) استخدامًا شبيهًا باستخدام apt-get؛ فلتثبيت حزمة nmap مع جميع الاعتماديات اللازمة، كما في مثال apt-get، فسنستخدم الأمر الآتي:

```
sudo aptitude install nmap
```

ولحذف نفس الحزمة، سنستخدم الأمر:

```
sudo aptitude remove nmap
```

راجع صفحات الدليل man لمزيد من المعلومات حول الخيارات السطرية للأداة aptitude.

٥. التحديثات التلقائية

يمكن استخدام الحزمة unattended-upgrades لتثبيت تحديثات الحزم تلقائيًا، ويمكن ضبطها لتحديث كل الحزم، أو تثبيت التحديثات الأمنية فقط؛ لكن أولًا يجب تثبيت الحزمة بإدخال الأمر الآتي في الطرفية:

```
sudo apt-get install unattended-upgrades
```

لضبط unattended-upgrades، عدِّل مما يلي في الملف التالي:

```
vim /etc/apt/apt.conf.d/50unattended-upgrades
```

ليوافق ما تحتاج:

```
Unattended-Upgrade::Allowed-Origins {
        "Ubuntu trusty-security";
//      "Ubuntu trusty-updates";
};
```

ويمكن أيضًا وضع بعض الحزم في «القائمة السوداء» مما يؤدي إلى عدم تحديثها تلقائيًّا؛ لإضافة حزمة ما إلى القائمة السوداء:

```
Unattended-Upgrade::Package-Blacklist {
//        "vim";
//        "libc6";
//        "libc6-dev";
//        "libc6-i686";
};
```

ملاحظة: الإشارة «//» تعمل كتعليق (comment)، أي أن كل ما يتبع // لن يُفسَّر.

لتفعيل التحديثات التلقائية، عدِّل ملف /etc/apt/apt.conf.d/10periodic واضبط إعدادات apt المناسبة:

```
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Download-Upgradeable-Packages "1";
APT::Periodic::AutocleanInterval "7";
APT::Periodic::Unattended-Upgrade "1";
```

الضبط السابق يُحدِّث فهرس الحزم ويُنزِّل ويُثبِّت جميع الترقيات المتوفرة كل يوم و«يُنظِّف» أرشيف التنزيل المحلي كل أسبوع.

ملاحظة: يمكنك قراءة المزيد عن خيارات ضبط apt الزمنية في ترويسة سكربت /etc/cron.daily/apt.

سيُسجِّل ناتج unattended-upgrades إلى ملف /var/log/unattended-upgrades.

ا. الإشعارات

ضبط المتغير Unattended-Upgrade::Mail في ملف /etc/apt/apt.conf.d/50unattended-upgrades سيجعل unattended-upgrades يرسل بريدًا إلكترونيًا إلى مدير النظام يُفصِّل فيه الحزم التي تحتاج إلى ترقية، أو التي تتعرض لمشاكل.

حزمة أخرى مفيدة هي apticron، التي تضبط عملًا مجدولًا (cron) لإرسال بريد إلكتروني لمدير النظام، يحتوي على معلومات حول أيّة حزم في النظام لها تحديثات متوفرة، وملخص عن التغيرات في كل حزمة.

أدخِل الأمر الآتي في سطر الأوامر لتثبيت حزمة apticron:

```
sudo apt-get install apticron
```

بعد انتهاء تثبيت الحزمة، عدِّل الملف /etc/apticron/apticron.conf لضبط عنوان البريد الإلكتروني والخيارات الأخرى:

```
EMAIL="root@example.com"
```

٦. الضبط

الضبط الخاص بمستودعات أداة التحزيم المتقدمة (APT) مُخزَّنٌ في ملف /etc/apt/sources.list ومجلد /etc/apt/sources.list.d، ستُذكَر معلومات عن طريقة إضافة أو إزالة المستودعات من الملف في هذا القسم.

بإمكانك تعديل الملف لتفعيل المستودعات أو تعطيلها؛ على سبيل المثال، لتعطيل ضرورة إدراج القرص المضغوط الخاص بأوبنتو في كل مرة تُجرى فيها عملية على الحزم، فضع رمز التعليق قبل السطر الموافق لقرص CD-ROM، الذي يظهر في أول الملف:

```
# no more prompting for CD-ROM please
# deb cdrom:[Ubuntu 14.04 _Trusty Tahr_ - Release i386
↪ (20111013.1)]/ trusty main restricted
```

ا. مستودعات إضافية

بالإضافة إلى مستودعات الحزم الرسمية المدعومة المتوفرة لأوبنتو، هنالك مستودعات مصانة من المجتمع تمنحك إمكانية تثبيت الآلاف من الحزم الإضافية، أشهر اثنين منها هما مستودعا «Universe» و «Multiverse»، هذان المستودعان غير مدعومين من أوبنتو رسميًا؛ لكنهما مصانان من المجتمع، حيث يوفران حزمًا آمنة لاستخدامها على حاسوبك.

ملاحظة: قد يكون في الحزم الموجودة في مستودع «Multiverse» مشاكلٌ في الترخيص مما يمنع من توزيعها مع نظام التشغيل الحر، وقد يكونون غير قانونيين في منطقتك.

تحذير: لاحظ أن أيًّا من مستودعي «Universe» و «Multiverse» لا يحتويان حزمًا مدعومةً رسميًا من أوبنتو، وهذا يعني أنها قد لا تكون هنالك تحديثات أمنية لتلك الحزم.

هنالك مصادر عديدة للحزم، وأحيانًا توفر تلك المصادر حزمةً واحدةً فقط، في هذه الحالة، تكون مصادر الحزمة موفرة من مطور تطبيق واحد؛ يجب أن تكون حذرًا جدًا عند استخدام مصادر غير قياسية للحزم؛ وعليك -على أي حال- البحث عن المصدر جيدًا قبل القيام بأية عملية تثبيت، فقد تجعل بعض تلك الحزم من النظام غير مستقرٍ أو لا يؤدي وظائفه في بعض الجوانب.

تكون مستودعات «Universe» و «Multiverse» مفعَّلة افتراضيًا، لكن إذا أردت تعطيلها، فعدّل الملف /etc/apt/sources.list وضَعْ تعليقًا قبل الأسطر الآتية:

```
deb http://archive.ubuntu.com/ubuntu trusty universe multiverse
deb-src http://archive.ubuntu.com/ubuntu trusty universe
multiverse

deb http://us.archive.ubuntu.com/ubuntu/ trusty universe
deb-src http://us.archive.ubuntu.com/ubuntu/ trusty universe
deb http://us.archive.ubuntu.com/ubuntu/ trusty-updates
universe
deb-src http://us.archive.ubuntu.com/ubuntu/ trusty-updates
universe

deb http://us.archive.ubuntu.com/ubuntu/ trusty multiverse
deb-src http://us.archive.ubuntu.com/ubuntu/ trusty multiverse
deb http://us.archive.ubuntu.com/ubuntu/ trusty-updates
multiverse
deb-src http://us.archive.ubuntu.com/ubuntu/ trusty-updates
multiverse

deb http://security.ubuntu.com/ubuntu trusty-security universe
deb-src http://security.ubuntu.com/ubuntu trusty-security
universe
deb http://security.ubuntu.com/ubuntu trusty-security
multiverse
deb-src http://security.ubuntu.com/ubuntu trusty-security
multiverse
```

٧. مصادر

أغلبية المعلومات التي أُعطِيت في هذا الفصل موجودةٌ في صفحات الدليل، التي يتوفر كثير منها على الإنترنت:

- صفحة ويكي أوبنتو «InstallingSoftware» فيها بعض المعلومات.
- للمزيد من التفاصيل عن dpkg، راجع صفحة الدليل man dpkg.

- مقالة «APT HOWTO»، وصفحة الدليل man apt-get، توفر معلومات مفيدة عن كيفية استخدام apt-get.
- راجع صفحة الدليل man aptitude للمزيد من الخيارات الخاصة بأداة Aptitude.
- صفحة ويكي أوبنتو «Adding Repositories HOWTO» تحتوي معلومات مفيدة عن طريقة إضافة المستودعات.

٤

الشبكات

تتكون الشبكات من جهازين أو أكثر، كأنظمة الحواسيب والطابعات وغيرها من المعدات المتعلقة بها والتي يمكن أن تتصل إما باستخدام كبل فيزيائي أو بالروابط اللاسلكية؛ وذلك لمشاركة وتوزيع المعلومات بين الأجهزة المتصلة.

يوفر هذا الفصل معلوماتٍ عامة وأخرى متخصصة تتعلق بالشبكات، وتتضمن لمحةً عن مفاهيم الشبكة، ونقاشًا مفصَّلًا عن بروتوكولات الشبكة الشائعة.

١. ضبط الشبكة

تأتي أوبنتو مع عدد من الأدوات الرسومية لضبط أجهزة الشبكة، هذا الكتاب موجَّه لمدراء الخواديم، وسيُركِّز على إدارة الشبكة من سطر الأوامر.

ا. بطاقات إيثرنت

تُعرَّف بطاقات إيثرنت (Ethernet interfaces) في النظام باستخدام الاسم الاصطلاحي ethX، حيث تمثل X قيمةً رقميةً، وتُعرَّف أول بطاقة إيثرنت بالاسم eth0، والثانية بالاسم eth1، وهلُمَّ جرًا للبقية، حيث تُرتَّب ترتيبًا رقميًا.

التعرف على بطاقات إيثرنت

يمكنك استخدام الأمر ifconfig كما يلي للتعرف على جميع بطاقات إيثرنت بسرعة:

```
ifconfig -a | grep eth
eth0 Link encap:Ethernet HWaddr 00:15:c5:4a:16:5a
```

برمجيـةٌ أخرى تساعدك في التعرف على جميع بطاقات الشبكة المتوفرة في نظامك هي الأمر lshw؛ يُظهِر الأمر lshw في المثال الآتي بطاقة إيثرنت واحدة باسمها المنطقي eth0، مع معلومات الناقل (bus) وتفاصيل التعريف وكل الإمكانيات المدعومة:

```
sudo lshw -class network
  *-network
       description: Ethernet interface
       product: BCM4401-B0 100Base-TX
       vendor: Broadcom Corporation
       physical id: 0
       bus info: pci@0000:03:00.0
       logical name: eth0
       version: 02
       serial: 00:15:c5:4a:16:5a
       size: 10MB/s
       capacity: 100MB/s
       width: 32 bits
       clock: 33MHz
       capabilities: (snipped for brevity)
       configuration: (snipped for brevity)
       resources: irq:17 memory:ef9fe000-ef9fffff
```

الأسماء المنطقية لبطاقات إيثرنت

تُعـرَّف الأسـماء المنطقيـة للبطاقـات فـي الملـف /etc/udev/rules.d/70-persistent-net.rules، إذا أردت التحكم في بطاقة التي ستحصل على اسم منطقي معين، فـابحث عـن السـطر الـذي يطـابق عنـوان MAC الفيزيـائي للبطاقـة، وعـدِّل قيمـة NAME=ethX إلـى الاسـم المنطقي المطلوب؛ أعد إقلاع النظام لتطبيق التغيرات التي أجريتها.

إعدادات بطاقة إيثرنت

إن ethtool هـو برنامـج يُظهِـر ويعـدِّل إعـدادات بطاقـة إيـثرنت كالمفاوضـة التلقائيـة (auto-negotiation)، وسـرعة المنفـذ، ونمـط duplex (اتصـال باتجـاه وحيـد، أم باتجـاهين)، وخاصية الاستيقاظ عند وصول إشارة معينة من شبكة WoL (Wake-on-LAN)؛ هذا البرنامج غير مثبَّت افتراضيًا، لكنه متوفر في المستودعات للتثبيت:

```
sudo apt-get install ethtool
```

ما يلي مثالٌ عن عرض الميزات المدعومة، وضبط إعدادات بطاقة إيثرنت:

```
sudo ethtool eth0
Settings for eth0:
    Supported ports: [ TP ]
    Supported link modes:  10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Half 1000baseT/Full
    Supports auto-negotiation: Yes
    Advertised link modes: 10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Half 1000baseT/Full
    Advertised auto-negotiation: Yes
    Speed: 1000Mb/s
    Duplex: Full
    Port: Twisted Pair
    PHYAD: 1
    Transceiver: internal
    Auto-negotiation: on
    Supports Wake-on: g
    Wake-on: d
    Current message level: 0x000000ff (255)
    Link detected: yes
```

التغيرات التي أُجريت بالأداة ethtool هي تغيرات مؤقتة، وستزول بعد إعادة الإقلاع، إذا أردت الحفاظ على تلك الخيارات، فأضف أمر ethtool الذي تريده إلى عبارة pre-up (التي تُنفَّذ عند تهيئة البطاقة وقبل استخدامها)، في ملف الإعدادات /etc/network/interfaces.

يوضح المثال الآتي كيف يمكن ضبط إعدادات بطاقة مُعرَّفة على أنها eth0 بسرعة منفذ تساوي 1000Mb/s وتعمل في نمط full duplex (اتصال باتجاهين):

```
auto eth0
iface eth0 inet static
pre-up /sbin/ethtool -s eth0 speed 1000 duplex full
```

ملاحظة: على الرغم من أن المثال السابق يستخدم الطريقة «static»، إلا أنه يعمل مع الطرق الأخرى أيضًا، كاستخدام DHCP؛ فالغرض من المثال السابق هو توضيح المكان الصحيح لوضع عبارة pre-up في ملف إعدادات البطاقة وحسب.

ب. عناوين IP

سيشرح القسم الآتي طريقة إعداد عناوين IP لنظامك، وضبط البوابة (gateway) الافتراضية اللازمة للتواصل على الشبكة المحلية والإنترنت.

إسناد مؤقت لعنوان IP

يمكن استخدام الأوامر القياسية عند الضبط المؤقت للشبكة، كالأمر ip و ifconfig و route التي يمكنك إيجادها في أغلب أنظمة تشغيل غنو/لينُكس؛ تسمح لك هذه الأوامر بضبط الإعدادات التي تأخذ حيز التنفيذ فوريًا، لكنها ليست دائمة؛ أي أنها لن تبقى مُفعَّلةً بعد إعادة التشغيل.

لضبط عنوان IP مؤقتًا، استخدم الأمر **ifconfig** بالطريقة الآتية: لتعديل عنوان IP وقناع الشبكة الفرعية (subnet mask) لمطابقة متطلبات الشبكة:

```
sudo ifconfig eth0 10.0.0.100 netmask 255.255.255.0
```

للتأكد من ضبط عنوان IP للبطاقة eth0:

```
ifconfig eth0
eth0          Link encap:Ethernet   HWaddr 00:15:c5:4a:16:5a
              inet addr:10.0.0.100 Bcast:10.0.0.255
Mask:255.255.255.0
              inet6 addr: fe80::215:c5ff:fe4a:165a/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:466475604 errors:0 dropped:0 overruns:0
frame:0
              TX packets:403172654 errors:0 dropped:0 overruns:0
carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:2574778386 (2.5 GB)  TX bytes:1618367329
(1.6 GB)
              Interrupt:16
```

لضبط البوابة الافتراضية، يمكنك استخدام الأمر **route** بالطريقة الآتية: حيث عليك تغيير عنوان البوابة الافتراضية لمطابقة متطلبات شبكتك:

```
sudo route add default gw 10.0.0.1 eth0
```

يمكنك استخدام الأمر route بهذه الطريقة للتأكد من ضبط البوابة الافتراضية:

```
route -n
Kernel IP routing table
Destination   Gateway   Genmask         Flags Metric Ref Use Iface
10.0.0.0      0.0.0.0   255.255.255.0   U     1      0   0   eth0
0.0.0.0       10.0.0.1  0.0.0.0         UG    0      0   0   eth0
```

إذا كنت تحتاج إلى DNS لإعدادات شبكتك المؤقتة، فيمكنك إضافة عناوين IP لخواديم DNS في الملف /etc/resolv.conf، لكن ليس من المستحسن عمومًا تعديل الملف /etc/resolv.conf مباشرةً، لكن هذا ضبط مؤقت وغير دائم؛ يوضح المثال الآتي طريقة إضافة عناوين خادومَي DNS إلى ملف /etc/resolv.conf؛ التي يجب أن تُبدَّل إلى الخواديم الملائمة لشبكتك؛ شرحٌ مطول عن ضبط إعدادات عميل DNS سيأتي في القسم الآتي.

```
nameserver 8.8.8.8
nameserver 8.8.4.4
```

إذا لم تعد بحاجة لهذا الضبط وتريد مسح كل إعدادات IP من بطاقة معينة، فعليك استخدام الأمر ip مع الخيار flush كما يلي:

```
ip addr flush eth0
```

ملاحظة: عملية إزالة ضبط IP باستخدام الأمر ip لا تمسح محتويات ملف /etc/resolv.conf، فعليك حذف أو تعديل محتوياته يدويًا.

إسناد ديناميكي لعنوان IP (عميل DHCP)

لإعداد الخادوم لكي يستخدم DHCP لإسناد العنوان ديناميكيًا، فأضف الطريقة dhcp إلى عبارة «عائلة العنوان» (address family) inet للبطاقة المطلوبة في ملف /etc/network/interfaces، يفترض المثال الآتي أنك تُعِدّ بطاقة إيثرنت الأولى المعرَّفة باسم eth0:

```
auto eth0
iface eth0 inet dhcp
```

بإضافة ضبط للبطاقة كما في المثال السابق، يمكنك أن تفعّل البطاقة باستخدام الأمر ifup الذي يهيّء DHCP باستخدام dhclient.

```
sudo ifup eth0
```

لتعطيل البطاقة يدويًا، يمكنك استخدام الأمر ifdown، الذي بدوره يهيّء عملية الإطلاق (release) الخاصة بنظام DHCP، ويوقف عمل البطاقة.

```
sudo ifdown eth0
```

إسناد عنوان IP ثابت

لإعداد نظامك لاستخدام عنوان IP ثابت، فاستخدم الطريقة static في عبارة «عائلة العنوان» في inet للبطاقة المطلوبة في ملف /etc/network/interfaces، يفترض المثال الآتي أنك تُعِدّ بطاقة إيثرنت الأولى المعرَّفة باسم eth0.

عدِّل العنوان (address) وقناع الشبكة (netmask) والبوابة (gateway) إلى القيم التي تتطلبها شبكتك:

```
auto eth0
iface eth0 inet static
address 10.0.0.100
netmask 255.255.255.0
gateway 10.0.0.1
```

بعد إضافة ضبط للبطاقة كما في المثال السابق، يمكنك أن تفعِّل البطاقة باستخدام الأمر ifup:

```
sudo ifup eth0
```

يمكنك استخدام الأمر ifdown لتعطيل البطاقة يدويًا:

```
sudo ifdown eth0
```

بطاقة loopback

إن بطاقة loopback (التي هي المضيف المحلي)، معرَّفة من النظام بالاسم lo، ولها عنوان IP الافتراضي 127.0.0.1، ويمكن أن تُعرَض باستخدام الأمر ifconfig:

```
ifconfig lo
lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING    MTU:16436  Metric:1
          RX packets:2718 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2718 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:183308 (183.3 KB)   TX bytes:183308 (183.3 KB)
```

افتراضيًا، يجب أن يكون هنالك سطران في ملف /etc/network/interfaces مسؤولان عن ضبط بطاقة loopback تلقائيًا، ومن المستحسن أن تبقي على الإعدادات الافتراضية ما لم يكن لك غرضٌ محدد من تغييرها؛ مثال على السطرين الافتراضيين:

```
auto lo
iface lo inet loopback
```

ج. استبيان الأسماء

إن استبيان الأسماء (Name resolution) الذي يتعلق بشبكات IP، هو عملية ربط عناوين IP إلى أسماء المضيفين، جاعلًا من السهل تمييز الموارد على الشبكة؛ سيشرح القسم الآتي كيف يُعَدّ النظام لاستبيان الأسماء باستخدام DNS، وسجلات أسماء المضيفين الثابتة (static hostname records).

ضبط إعدادات عميل DNS

تقليديًا، كان الملف /etc/resolv.conf ملف ضبطٍ ثابتٍ لا تحتاج لتعديله إلا نادرًا، أو كان يُعدَّل تلقائيًا عبر عميل DHCP؛ أما حاليًا فيمكن أن يُبدِّل الحاسوب بين شبكةٍ وأخرى من حين لآخر، وأصبح يُستخدَم إطار العمل resolvconf لتَتَبُّع هذه التغيرات وتحديث إعدادات استبيان الأسماء تلقائيًا؛ في الواقع هو وسيط بين البرامج التي توفر معلومات استبيان الأسماء، والتطبيقات التي تحتاج إلى تلك المعلومات.

يُغَذّى Resolvconf بالمعلومات عبر مجموعة من السكربتات التي تتعلق بإعدادات بطاقة الشبكة، الفرق الوحيد بالنسبة للمستخدم هي أن أيّة تعديلات حدثت على ملف /etc/resolv.conf ستُفقَد عندما تُعاد كتابته كل مرة يُشغِّل فيها حدثٌ ما resolvconf؛ فبدلًا من ذلك، يستخدم resolvconf عميل DHCP وملف /etc/network/interfaces لتوليد قائمة بخواديم الأسماء والنطاقات ليضعها في ملف /etc/resolv.conf، الذي هو الآن وصلةٌ رمزية (symlink):

```
/etc/resolv.conf -> ../run/resolvconf/resolv.conf
```

لضبط استبيان الأسماء، أضف عناوين IP لخواديم الأسماء الملائمة لشبكتك في ملف /etc/network/interfaces، يمكنك إضافة قائمة بحث اختيارية للاحقة DNS (DNS suffix search-lists) لمطابقة أسماء نطاقات الشبكة، ولكل خيار ضبط resolv.conf صالح، يمكنك تضمين سطر واحد يبدأ باسم الخيار مع السابقة -dns مما ينتج ملفًا شبيهًا بالملف الآتي:

```
iface eth0 inet static
      address 192.168.3.3
      netmask 255.255.255.0
      gateway 192.168.3.1
      dns-search example.com
      dns-nameservers 192.168.3.45 192.168.8.10
```

يمكن أن يُستخدَم الخيار search مع عدّة أسماء نطاقات، وستُلحَق طلبيات DNS في التسلسل الذي أُدخِلَت به؛ على سبيل المثال، ربما يكون لشبكتك نطاقات فرعية يجب البحث فيها؛ نطاق رئيسي «example.com»، ونطاقين فرعيين «sales.example.com» و «dev.example.com».

إذا كنت تريد البحث في عدّة نطاقات فرعية، فسيكون ملف الضبط كالآتي:

```
iface eth0 inet static
      address 192.168.3.3
      netmask 255.255.255.0
      gateway 192.168.3.1
      dns-search example.com sales.example.com dev.example.com
      dns-nameservers 192.168.3.45 192.168.8.10
```

إذا كنت تحاول عمل ping للمضيف ذي الاسم server1، فسيطلب النظام تلقائيًا طلبية DNS لاسم النطاق الكامل (Fully Qualified Domain Name [FQDN])، في الترتيب الآتي:

١. server1.example.com

٢. server1.sales.example.com

٣. server1.dev.example.com

إذا لم يُعثَر على أيّة مطابقات، فسيزودنا خادوم DNS بنتيجة «notfound»، وستفشل طلبية DNS.

أسماء المضيفين الثابتة

يمكن تعريف أسماء ثابتة للمضيفين تربط بين اسم المضيف وعنوان IP في ملف /etc/hosts؛ المدخلات في ملف hosts ستسبق طلبيات DNS افتراضيًا، هذا يعني لو أن نظامك حاول تفسير اسم مضيف، وكان هذا الاسم يطابق مدخلةً في ملف /etc/hosts، فلن يحاول البحث في سجلات DNS؛ وفي بعض حالات الاستخدام -وخصوصًا عندما لا يُتَطَّلب الوصول إلى الإنترنت- يمكن أن تتعرف الخواديم الموصولة بعدد قليل من الموارد الشبكية على بعضها باستخدام أسماء المضيفين الثابتة بدلًا من DNS.

المثال الآتي هو ملف hosts، حيث نجد عددًا من الخواديم المحلية قد عُرِّفَت بأسماء مضيفين بسيطة، وأسماءٍ بديلة، وأسماء النطاقات الكاملة المكافئة لها:

```
127.0.0.1 localhost
127.0.1.1 ubuntu-server
10.0.0.11 server1 vpn server1.example.com
10.0.0.12 server2 mail server2.example.com
10.0.0.13 server3 www server3.example.com
10.0.0.14 server4 file server4.example.com
```

ملاحظة: لاحظ أن كل خادوم من الخواديم في المثال السابق قد أُعطي أسماءً بديلةً بالإضافة إلى أسمائها الأساسية، وأسماء النطاقات الكاملة؛ حيث رُبِطَ server1 مع الاسم vpn، و server2 يُشار إليه بالاسم mail، و server3 بالاسم www، و server4 بالاسم file.

ضبط تبديل خدمة الأسماء

الترتيب الذي يتبّعه نظامك لاختيار طريقةٍ لتحويل أسماء المضيفين إلى عناوين IP مُتَحَكَّمٌ به من ملف إعدادات «مُبَدِّل خدمة الأسماء» (Name Service Switch [NSS]) الموجود في /etc/nsswitch.conf؛ وكما ذُكِرَ في القسم السابق، فإن أسماء المضيفين الثابتة المعرَّفة في ملف /etc/hosts تسبق استخدام سجلات DNS؛ المثال الآتي يحتوي على السطر المسؤول عن ترتيب البحث عن أسماء المضيفين في ملف /etc/nsswitch.conf:

```
hosts: files mdns4_minimal [NOTFOUND=return] dns mdns4
```

- files: المحاولة أولًا للحصول على العناوين من ملف أسماء المضيفين الثابتة في /etc/hosts.
- mdns4_minimal: محاولة الحصول على العناوين باستخدام Mulitcast DNS.
- [NOTFOUND=return]: تعني أن أي جواب يكون notfound أتى من عملية mdns4_minimal السابقة سيُعامَل بموثقية، ولن يحاول النظام الاستمرار في محاولة الحصول على جواب.
- dns: تمثل طلبية Unicast DNS قديمة.
- mdns4: تمثل طلبية Mulitcast DNS.

لتعديل ترتيب طرائق استبيان الأسماء (name resolution) المذكورة آنفًا، يمكنك بكل بساطة تعديل قيمة عبارة «hosts» للقيمة التي تريدها؛ على سبيل المثال، لو كنت تفضل استخدام Unicast DNS القديم، بدلًا من Mulitcast DNS، فتستطيع تغيير تلك السلسلة النصية في ملف /etc/nsswitch.conf كما يلي:

```
hosts: files dns [NOTFOUND=return] mdns4_minimal mdns4
```

د. إنشاء الجسور

إنشاء جسر (bridge) بين عدة بطاقات شبكية هو ضبط متقدم جدًا، لكنه مفيد كثيرًا في حالات عديدة، أحد تلك الحالات هو إنشاء جسر بين عدة اتصالات شبكية، ثم استخدام جدار ناري لترشيح (filter) ما يمر بين قسمين من الشبكة؛ حالةٌ أخرى هي استخدام إحدى البطاقات لتمكين «الآلات الوهمية» (Virtual Machines) من الوصول إلى الشبكة الخارجية؛ يشرح المثال الآتي الحالة الأخيرة.

قبل ضبط إعدادات الجسر، عليك تثبيت حزمة bridge-utils، أدخِل الأمر الآتي في الطرفية لتثبيت هذه الحزمة:

```
sudo apt-get install bridge-utils
```

ثم اضبط الجسر بتعديل ملف /etc/network/interfaces:

```
auto lo
iface lo inet loopback

auto br0
iface br0 inet static
      address 192.168.0.10
      network 192.168.0.0
      netmask 255.255.255.0
      broadcast 192.168.0.255
      gateway 192.168.0.1
      bridge_ports eth0
      bridge_fd 9
      bridge_hello 2
      bridge_maxage 12
      bridge_stp off
```

ملاحظة: أدخِل القيم الملائمة لبطاقتك الفيزيائية، والشبكة عندك.

ثم شغِّل بطاقة الجسر:

```
sudo ifup br0
```

يجب أن تعمل بطاقة الجسر تلقائيًا الآن، تُوفِّر الأداة brctl معلوماتٍ حول حالة الجسر، وتتحكم بالبطاقات التي تكوِّن جزءًا من الجسر؛ راجع صفحة الدليل man brctl لمزيد من المعلومات.

٥. مصادر

- هنالك وصلات في صفحة ويكي أوبنتو «Network» تشير إلى مقالات تشرح الضبط المتقدم جدًا للشبكة.
- صفحة الدليل الخاصة بالبرمجية resolvconf فيها بعض المعلومات عن resolvconf.
- صفحة دليل man interfaces تحتوي على تفاصيل عن خياراتٍ أخرى لملف /etc/network/interfaces.
- صفحة دليل man dhclient تحتوي على تفاصيل عن الخيارات الأخرى لضبط إعدادات عميل DHCP.
- للمزيد من المعلومات حول ضبط عميل DNS، راجع صفحة الدليل man resolver؛ راجع أيضًا الفصل السادس من الكتاب المنشور من O'Reilly: «Linux Network Administrator's Guide»؛ الذي هو مصدر جيد للمعلومات حول ضبط resolver، وخدمة الأسماء.
- لمزيد من المعلومات حول الجسور، راجع صفحة الدليل man brctl، وصفحة Networking-bridge في موقع مؤسسة لينُكس (Linux Foundation).

٢. بروتوكول TCP/IP

إن بروتوكول التحكم في نقل البيانات (Transmission Control Protocol) وبروتوكول الإنترنت (Internet Protocol) المسمى اختصارًا TCP/IP هو معيار يضم مجموعة بروتوكولاتٍ مطورةً في نهاية السبعينات من القرن الماضي من وكالة مشاريع أبحاث الدفاع المتقدمة (Defense Advanced Research Projects Agency [DARPA])، كطرق للتواصل بين مختلف أنواع الحواسيب وشبكات الحواسيب؛ إن بروتوكول TCP/IP هو العصب المحرك للإنترنت، وهذا ما يجعله أشهر مجموعة بروتوكولات شبكيّة على وجه الأرض.

ا. مقدمة عن TCP/IP

المكونان الرئيسيان من مكونات TCP/IP يتعاملان مع مختلف نواحي شبكة الحاسوب؛ بروتوكول الإنترنت -جزء «IP» من TCP/IP- هو بروتوكول عديم الاتصال (connectionless) يتعامل مع طريقة توجيه (routing) الرزم الشبكية مستخدمًا ما يسمى «IP Datagram» كوحدة رئيسية للمعلومات الشبكية؛ تتكون IP Datagram من ترويسة، يتبعها رسالة. إن بروتوكول التحكم في نقل البيانات هو «TCP» من TCP/IP، ويُمكِّن مضيفي الشبكة من إنشاء اتصالاتٍ يستطيعون استخدامها لتبادل مجاري البيانات (data streams)؛ ويَضمَن أيضًا بروتوكول TCP أن البيانات التي أُرسِلَت بواسطة تلك الاتصالات ستُسَلَّم وتصل إلى مضيف الشبكة المُستقبِل كما أُرسِلَت تمامًا وبنفس الترتيب من المُرسِل.

ب. ضبط TCP/IP

يتكون ضبط TCP/IP من عدّة عناصر التي يمكن أن تُغيَّر بتعديل ملفات الإعدادات الملائمة، أو باستخدام حلول مثل خادوم «بروتوكول ضبط المضيف الديناميكي» (Dynamic Host Configuration Protocol [DHCP])، الذي يمكن أن يُضبَط لتوفير إعدادات TCP/IP صالحة لعملاء الشبكة تلقائيًا، يجب أن تُضبط قيم تلك الإعدادات ضبطًا صحيحًا لكي تساعد في عمل الشبكة عملًا سليمًا في نظام أوبنتو عندك.

عناصر الضبط الخاصة ببروتوكول TCP/IP ومعانيها هي:

- عنوان IP: هو سلسلة نصية فريدة يُعبَّر عنها بأربع مجموعات من أرقام تتراوح بين الصفر (٠)، ومئتان وخمسٌ وخمسون (٢٥٥)، مفصولةٌ بنقط، وكل أربعة أرقام تمثل ثمانية (٨) بتات من العنوان الذي يكون طوله الكامل اثنان وثلاثون (٣٢) بتًا، تُسمى هذه الصيغة باسم «dotted quad notation».

- قناع الشبكة: قناع الشبكة الفرعية (أو باختصار: قناع الشبكة [netmask])، هو قناع ثنائي يفصل قسم عنوان IP المهم للشبكة، عن قسم العنوان المهم للشبكة الفرعية (Subnetwork)؛ على سبيل المثال، في شبكة ذات الفئة C (Class C network)، قناع الشبكة الافتراضي هو 255.255.255.0، الذي يحجز أول ثلاثة بايتات من عنوان IP للشبكة، ويسمح لآخر بايت من عنوان IP أن يبقى متاحًا لتحديد المضيفين على الشبكة الفرعية.

- عنوان الشبكة: يمثل عنوان الشبكة (Network Address) البايتات اللازمة لتمثيل الجزء الخاص من الشبكة من عنوان IP، على سبيل المثال، المضيف صاحب العنوان 12.128.1.2 في شبكة ذات الفئة A يستطيع استخدام 12.0.0.0 كعنوان الشبكة، حيث يمثل الرقم ١٢ البايت الأول من عنوان IP (جزء الشبكة)، وبقية الأصفار في البايتات الثلاثة المتبقية تمثل قيم مضيفين محتملين في الشبكة؛ وفي مضيف شبكة يستخدم عنوان IP الخاص 192.168.1.100 الذي يستخدم بدوره عنوان الشبكة .192 168.1.0 الذي يحدد أول ثلاثة بايتات من شبكة ذات الفئة C والتي هي 192.168.1، وصفرًا الذي يُمثِّل جميع القيم المحتملة للمضيفين على الشبكة.

- عنوان البث: عنوان البث (Broadcast Address) هو عنوان IP يسمح لبيانات الشبكة بأن تُرسَل إلى كل المضيفين معًا في شبكة محلية بدلًا من إرسالها لمضيف محدد. العنوان القياسي العام للبث لشبكات IP هو 255.255.255.255، لكن لا يمكن استخدام هذا العنوان لبث الرسائل لكل مضيف على شبكة الإنترنت، لأن الموجهات (routers) تحجبها؛ ومن الملائم أن يُضبَط عنوان البث لمطابقة شبكة فرعية محددة، على سبيل المثال، في شبكة خاصة ذات الفئة C، أي 192.168.1.0، يكون عنوان البث 192.168.1 .255؛ تُولَّد رسائل البث عادةً من بروتوكولات شبكيّة مثل بروتوكول استبيان العناوين (Address Resolution Protocol [ARP])، وبروتوكول معلومات التوجيه (Routing Information Protocol [RIP]).

- عنوان البوابة: إن عنوان البوابة (Gateway Address) هو عنوان IP الذي يمكن الوصول عبره إلى شبكة معينة أو إلى مضيف معين على شبكة؛ فإذا أراد أحد مضيفي الشبكة التواصل مع مضيفٍ آخر، ولكن المضيف الآخر ليس على نفس الشبكة، فيجب عندئذٍ استخدام البوابة؛ في حالات عديدة، يكون عنوان البوابة في شبكةٍ ما هو الموجه (router) على تلك الشبكة، الذي بدوره يُمرِّر البيانات إلى بقية الشبكات أو المضيفين كمضيفي الإنترنت على سبيل المثال. يجب أن تكون قيمة عنوان البوابة صحيحةً، وإلا فلن يستطيع نظامك الوصول إلى أي مضيف خارج حدود شبكته نفسها.

- عنوان خادوم الأسماء: عناوين خادوم الأسماء (Nameserver Addresses) تمثل عناوين IP لخواديم خدمة أسماء المضيفين DNS، التي تستطيع استبيان (resolve) أسماء مضيفي الشبكة وتحويلها إلى عناوين IP؛ هنالك ثلاث طبقات من عناوين خادوم الأسماء، التي يمكن أن تُحدَّد بترتيب استخدامها: خادوم الأسماء الرئيسي (Primary)، وخادوم الأسماء الثانوي (Secondary)، وخادوم الأسماء الثلاثي (Tertiary)، ولكي يستطيع نظامك استبيان أسماء أسماء مضيفي الشبكة وتحويلها إلى عناوين IP الموافقة لهم، فيجب عليك تحديد عناوين خادوم الأسماء الذي تثق به لاستخدامه في ضبط TCP/IP لنظامك؛ في حالاتٍ عديدة، تُوفَّر هذه العناوين من موزع خدمة شبكتك، لكن هنالك خواديم أسماء عديدة متوفرة مجانًا للعموم، كخواديم Level3 (Verizon) بعناوين IP تتراوح بين 4.2.2.1 إلى 4.2.2.6.

تنبيه: إن عنوان IP، وقناع الشبكة، وعنوان الشبكة، وعنوان البث، وعنوان البوابة تُحدَّد عادةً بالإمكان الملائمة لها في ملف /etc/network/interfaces، عناوين خادوم الأسماء تُحدَّد عادة في قسم nameserver في ملف /etc/resolve.conf، للمزيد من المعلومات، راجع صفحة الدليل لكلٍ من interfaces و resolv.conf على التوالي وبالترتيب، وذلك بكتابة الأوامر الآتية في محث الطرفية:

للوصول إلى صفحة دليل interfaces، اكتب الأمر الآتي:

man interfaces

وللوصول إلى صفحة دليل resolv.conf:

man resolv.conf

ج. توجيه IP

يمثِّل توجيه IP ‏(IP Routing) الوسائل اللازمة لتحديد واكتشاف الطرق في شبكات TCP/IP بالإضافة إلى تحديد بيانات الشبكة التي ستُرسَل، يَستخدِم التوجيه ما يسمى «جداول التوجيه» (routing tables) لإدارة تمرير رزم بيانات الشبكة من مصدرها إلى وجهتها؛ وذلك عادة بواسطة عقد شبكيّة وسيطة تسمى «موجهات» (routers)؛ وهنالك نوعان رئيسيان من توجيه IP: التوجيه الثابت (static routing)، والتوجيه الديناميكي (dynamic routing).

يشتمل التوجيه الثابت على إضافة توجيهات IP يدويًّا إلى جدول توجيهات النظام، ويتم ذلك عادةً بتعديل جدول التوجيهات باستخدام الأمر route؛ يتمتع التوجيه الثابت بعدّة مزايا تميزه عن التوجيه الديناميكي، كسهولة استخدامه في الشبكات الصغيرة، وقابلية التوقع (يُحسَب جدول التوجيهات مسبقًا دائمًا، وهذا ما يؤدي إلى استخدام نفس المسار في كل مرة)، ويؤدي إلى حِملٍ قليل على الموجهات الأخرى ووصلات الشبكة نتيجةً لعدم استخدام بروتوكولات التوجيه الديناميكي؛ لكن يواجه التوجيه الثابت بعض الصعوبات أيضًا؛ فعلى سبيل المثال، التوجيهُ الثابتُ محدودٌ للشبكات الصغيرة، ولا يمكن أن يتوسَّع توسعًا سهلًا، ويصعب عليه التأقلم مع نقصان أو فشل معدات الشبكة في الطريق المسلوك نتيجةً للطبيعة الثابتة لذاك الطريق.

يُعتَمَد على التوجيه الديناميكي في الشبكات الكبيرة ذات احتمالات عديدة للطرق الشبكية المسلوكة من المصدر إلى الوجهة، وتُستخدَم بروتوكولات توجيه خاصة، كبروتوكول معلومات الموجه (Router Information Protocol [RIP])، الذي يتولّى أمر التعديلات التلقائية في جداول التوجيه، مما يجعل من التوجيه الديناميكي أمرًا ممكنًا؛ وللتوجيه الديناميكي مزايا عدّة عن التوجيه الثابت، كإمكانية التوسع بسهولة، والتأقلم مع نقصان أو فشل معدات الشبكة خلال الطريق المسلوك في الشبكة، بالإضافة إلى الحاجة لإعداداتٍ قليلةٍ نسبيًا لجداول التوجيه، لأن الموجهات تعلم عن وجود وتوفر بعضها بعضًا؛ وهذه الطريقة تمنع حدوث مشاكل في التوجيه نتيجةً لخطأ بشري في جداول التوجيه. لكن التوجيه الديناميكي ليس كاملًا، ويأتي مع عيوب، كالتعقيد، والحِمل الزائد على الشبكة بسبب التواصل بين الموجهات، التي لا تفيد المستخدمين المباشرين فوريًا، وتستهلك التراسل الشبكي.

د. بروتوكولَي TCP و UDP

إن بروتوكول TCP هو بروتوكول مبني على الاتصال (connection-based)، ويوفر آليةً لتصحيح الأخطاء، وضمانةً لتسليم البيانات عبر ما يُعرَف بالمصطلح «التحكم في الجريان» (flow control)، يُحدِّد التحكم في الجريان متى يجب إيقاف نقل البيانات، وإعادة إرسال الرزم التي أُرسِلَت سابقًا والتي واجهة مشاكل كالتصادمات (collisions)؛ إذ أنَّ التأكيد على الوصول الدقيق والكامل للبيانات عبر بروتوكول TCP هو أمر جوهري في عملية تبادل البيانات المهمة كالتحويلات في قواعد البيانات.

أما بروتوكول UDP ‏(User Datagram Protocol) على الجهة الأخرى، هو بروتوكول عديم الاتصال (connectionless)، الذي نادرًا ما يتعامل مع عمليات نقل البيانات المهمة لأنه يفتقر إلى التحكم في جريان البيانات أو أيّة طريقة أخرى للتأكد من توصيل البيانات عمليًا؛ لكن بروتوكول UDP يُستخدَم استخدامًا شائعًا في التطبيقات كتدفق (streaming) الصوت والصورة، حيث أنه أسرع بكثير من TCP لأنه لا يحتوي على آليةٍ لتصحيح الأخطاء والتحكم في الجريان، وفي الأماكن التي لا يهم فيها فقدان بعض الرزم الشبكية كثيرًا.

ه. بروتوكول ICMP

إن بروتوكول ICMP ‏(Internet Control Messaging Protocol) هو إضافة إلى بروتوكول الإنترنت (IP) الذي يُعرَّف في RFC ‏(Request For Comments) ذي الرقم 792# ويدعم التحكم في احتواء الرزم الشبكية والأخطاء ورسائل المعلومات، يُستخدَم بروتوكول ICMP بتطبيقات شبكيّة كأداة ping، التي تستطيع تحديد إذا ما كان جهازٌ ما متاحًا على الشبكة، أمثلة عن رسالة الخطأ المُعادَة من ICMP -التي تكون مفيدةً لمضيفي الشبكة وللأجهزة كالموجهات- تتضمن رسالتَي «Destination Unreachable» و «Time Exceeded».

و. العفاريت

العفاريت (Daemons) هي تطبيقات نظام خاصة التي تعمل عادةً عملًا دائمًا في الخلفية، وتنتظر طلبياتٍ للوظائف التي توفرها من التطبيقات الأخرى، يتمحور عمل العديد من العفاريت حول الشبكة، وبالتالي فإن عددًا كبيرًا من العفاريت التي تعمل في الخلفية في نظام أوبنتو تُوفِّر وظائف تتعلق بالشبكة؛ بعض الأمثلة عن عفاريت الشبكة تتضمن «عفريت بروتوكول نقل النص الفائق»

(HyperText Transport Protocol Daemon [httpd])، الـذي يـوفر وظيفـة خـادوم الـويب؛ و «عفريت الصدفة الآمنة» (Secure SHell Daemon [sshd])، الذي يـوفر طريقةً للدخول الآمن عـن بُعد وإمكانيـات نقل الملفات؛ و «عفريـت بروتوكـول الوصـول إلـى رسـائل الإنـترنت» (Internet Message Access Protocol Daemon [imapd]) الذي يوفر خدمات البريد الإلكتروني.

ز. مصادر

- تتوفر صفحات دليلٍ لبروتوكولي TCP و IP التي تحتوي على معلومات قيمّة.
- راجع أيضًا المصدر الآتي من IBM: «TCP/IP Tutorial and Technical Overview».
- مصدرٌ أخرى هو كتاب «TCP/IP Network Administration» من O'Reilly.

٣. بروتوكول ضبط المضيف ديناميكيًّا DHCP

إن بروتوكول ضبط المضيف ديناميكيًّا (Dynamic Host Configuration Protocol) هو خدمة شبكة تُفعِّل إسناد إعدادات الشبكة إلى الحواسيب المضيفة من خادوم بدلًا من إعداد كل مضيف شبكي يدويًا؛ حيث لا تملك الحواسيب المُعدَّة كعملاءٍ لخدمة DHCP أيّة تحكم بالإعدادات التي تحصل عليها من خادوم DHCP.

إن أشهر الإعدادات الموفَّرة من خادوم DHCP إلى عملاء DHCP تتضمن:

- عنوان IP وقناع الشبكة.
- عنوان IP للبوابة الافتراضية التي يجب استخدامها.
- عناوين IP لخواديم DNS التي يجب استعمالها.

لكن يمكن أيضًا أن يوفِّر خادوم DHCP خاصيات الضبط الآتية:

- اسم المضيف.
- اسم النطاق.
- خادوم الوقت.
- خادوم الطباعة.

من مزايا استخدام DHCP هو أن أي تغييرٍ في إعدادات الشبكة -على سبيل المثال تغيير عنوان خادوم DNS- سيتم في خادوم DHCP فقط، وسيُعاد ضبط جميع مضيفي الشبكة في المرة القادمة التي سيَطلُبُ فيها عملاء DHCP معلومات الإعدادات من خادوم DHCP؛ ويُسهِّل استعمال خادوم DHCP إضافة حواسيب جديدة إلى الشبكة، فلا حاجة للتحقق من توفر عنوان IP؛ وسيقل أيضًا التضارب في حجز عناوين IP.

يمكن أن يُوفِّر خادوم DHCP إعدادات الضبط باستخدام الطرق الآتية:

التوزيع اليدوي (Manual allocation) عبر عنوان MAC

تتضمن هذه الطريقة استخدام DHCP للتعرف على عنوان مميز لعتاد كل كرت شبكة متصل إلى الشبكة، ثم سيوفِّر إعدادات ضبطٍ ثابتةً في كل مرة يتصل فيها عميل DHCP إلى خادوم DHCP باستخدام بطاقة الشبكة المعيّنة مسبقًا؛ وهذا يضمن أن يُسنَد عنوان معيّن إلى بطاقةٍ شبكيّةٍ معيّنة وذلك وفقًا لعنوان MAC.

التوزيع الديناميكي (Dynamic allocation)

سيُسنِد خادوم DHCP -في هذه الطريقة- عنوان IP من مجموعة من العناوين (تسمى pool، أو في بعض الأحيان range أو scope) لمدة من الزمن (يسمى ذلك بالمصطلح lease) التي تُضبَط في الخادوم، أو حتى يخبر العميل الخادوم أنه لم يعد بحاجةٍ للعنوان بعد الآن؛ وسيحصل العملاء في هذه الطريقة على خصائص الضبط ديناميكيًّا وفق المبدأ «الذي يأتي أولًا، يُخدَّم أولًا»؛ وعندما لا يكون عميل DHCP متواجدًا على الشبكة لفترة محددة، فسينتهي وقت الضبط المخصص له، وسيعود العنوان المسند إليه إلى مجموعة العناوين لاستخدامه من عملاء DHCP الآخرين؛ أي أنَّه في هذه الطريقة، يمكن «تأجير» أو استخدام العنوان لفترة من الزمن؛ وبعد هذه المدة، يجب أن يطلب العميل من الخادوم أن يعيد تأجيره إياه.

التوزيع التلقائي (Automatic allocation)

سيُسنِد خادوم DHCP -في هذه الطريقة- عنوان IP إسنادًا دائمًا إلى جهاز معين، ويتم اختيار هذه العنوان من مجموعة العناوين المتوفرة؛ يُضبَط عادةً DHCP لكي يُسنِد عنوانًا مؤقتًا إلى الخادوم، لكن يمكن أن يسمح خادوم DHCP بزمن تأجير «لا نهائي».

يمكن اعتبار آخر طريقتين «تلقائيتَين»، لأنه في كل حالة يُسنِد خادوم DHCP العنوان دون تدخل إضافي مباشر، الفرق الوحيد بينهما هو مدة تأجير عنوان IP؛ بكلماتٍ أخرى، هل ستنتهي صلاحية عنوان العميل بعد فترة من الزمن أم لا.

يأتي أوبنتو مع خادوم وعميل DHCP، الخادوم هو dhcpd (dynamic host configuration protocol daemon)، والعميل الذي يأتي مع أوبنتو هو dhclient، ويجب أن يثبَّت على جميع الحواسيب التي تريدها أن تُعَدّ تلقائيًا، كلا البرنامجين سهلُ التثبيت، وسيبدآن تلقائيًا عند إقلاع النظام.

ا. التثبيت

اكتب الأمر الآتي في مِحَث الطرفية لتثبيت dhcpd:

```
sudo apt-get install isc-dhcp-server
```

ربما تحتاج إلى تغيير الضبط الافتراضي بتعديل ملف /etc/dhcp/dhcpd.conf ليلائم احتياجاتك والضبط الخاص الذي تريده.

ربما تحتاج أيضًا إلى تعديل /etc/default/isc-dhcp-server لتحديد البطاقات الشبكية التي يجب أن «يستمع» (listen) إليها عفريت dhcpd.

ملاحظة: رسالة عفريت dhcpd تُرسَل إلى syslog، انظر هناك لرسائل التشخيص.

ب. الضبط

ربما سيربكك ظهور رسالة خطأ عند انتهاء التثبيت، لكن الخطوات الآتية ستساعدك في ضبط الخدمة:

في الحالات الأكثر شيوعًا، كل ما تريد أن تفعله هو إسناد عناوين IP إسنادًا عشوائيًا، يمكن أن يُفعَل ذلك بالإعدادات الآتية:

```
# minimal sample /etc/dhcp/dhcpd.conf
default-lease-time 600;
max-lease-time 7200;

subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.150 192.168.1.200;
  option routers 192.168.1.254;
  option domain-name-servers 192.168.1.1, 192.168.1.2;
  option domain-name "mydomain.example";
}
```

نتيجة الإعدادات السابقة هي ضبط خادوم DHCP لإعطاء العملاء عناوين IP تتراوح من 192.168.1.150 إلى 192.168.1.200، وسيُأجَّر عنوان IP لمدة ٦٠٠ ثانية إذا لم يطلب العميل وقتًا محددًا؛ عدا ذلك، فسيكون وقت الإيجار الأقصى للعنوان هو ٧٢٠٠ ثانية؛ و«سينصح» الخادومُ العميلَ أن يستخدم 192.168.1.254 كبوابة افتراضية، و 192.168.1.1 و .192.168

1.2 كخادومَيّ DNS.

عليك إعادة تشغيل خدمة dhcpd بعد تعديل ملف الضبط:

```
sudo service isc-dhcp-server restart
```

ج. مصادر

- توجد بعض المعلومات المفيدة في صفحة ويكي أوبنتو «dhcp3-server».
- للمزيد من خيارات ملف /etc/dhcp/dhcpd.conf، راجع صفحة الدليل man dhcpd.conf.
- مقالة في ISC: «dhcp-server».

٤. مزامنة الوقت باستخدام بروتوكول NTP

إن بروتوكول NTP هو بروتوكول TCP/IP، يُستخدَم لمزامنة الوقت عبر الشبكة؛ بكلماتٍ بسيطة: يطلب العميل الوقت الحالي من الخادوم ثم يستخدمه لمزامنة ساعته الداخلية.

هنالك الكثير من التعقيدات خلف هذا التفسير البسيط، فهنالك درجات من خواديم NTP؛ فالدرجة الأولى من خواديم NTP تتصل بساعات ذريّة (atomic clock)، والدرجة الثانية والثالثة من الخواديم تُوزِّع الحِمل عبر الإنترنت؛ وحتى برمجية العميل هي برمجية معقدة أكثر بكثير مما تظن، فهنالك عامل لأخذ التأخير في الاتصالات بعين الاعتبار، وتعديل الوقت في طريقة لا تُفسِد وظيفة جميع العمليات التي تعمل في الخادوم؛ ولحسن الحظ أنَّ كل هذا التعقيد مخفيٌ عنك! تستخدم أوبنتو ntpdate، و ntpd.

ا. الأداة ntpdate

يأتي أوبنتو افتراضيًا مع الأداة ntpdate، وستعمل عند الإقلاع لتضبط وقتك وفقًا لخادوم NTP الخاص بأوبنتو:

```
ntpdate -s ntp.ubuntu.com
```

ب. عفريت ntpd

يحسب عفريت ntp الانزياح في ساعة وقت النظام، ويعدِّلها باستمرار، لذلك لن يكون هنالك تصحيحات كبيرة ستؤدي إلى اختلال في السجلات (logs) على سبيل المثال. لكن سيكون ثمن ذلك هو القليل من طاقة المعالجة والذاكرة، ولكن هذا لا يُذكَر بالنسبة إلى الخواديم الحديثة.

ج. التثبيت

لتثبيت ntpd، أدخل الأمر الآتي إلى الطرفية:

```
sudo apt-get install ntp
```

د. الضبط

عدِّل الملف /etc/ntp.conf لإضافة أو إزالة الأسطر التي تحتوي على عناوين الخواديم، تُضبَط هذه الخواديم افتراضيًا:

```
# Use servers from the NTP Pool Project. Approved by Ubuntu
Technical Board
# on 2011-02-08 (LP: #104525). See
http://www.pool.ntp.org/join.html for
# more information.
server 0.ubuntu.pool.ntp.org
server 1.ubuntu.pool.ntp.org
server 2.ubuntu.pool.ntp.org
server 3.ubuntu.pool.ntp.org
```

بعد تعديل ملف الضبط، عليك إعادة تحميل ntpd:

```
sudo service ntp reload
```

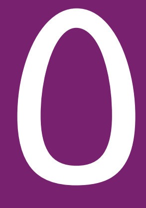
ه. مشاهدة الحالة

استخدم الأمر ntpq لرؤية المزيد من المعلومات:

```
sudo ntpq -p
remote           refid          st  t  when poll reach delay offset jitter
==============================================================================
+stratum2-2.NTP. 129.70.130.70   2  u  5    64   377   68.461 -44.274 110.334
+ntp2.m-online.n 212.18.1.106    2  u  5    64   377   54.629 -27.318  78.882
*145.253.66.170 .DCFa.           1  u  10   64   377   83.607 -30.159  68.343
+stratum2-3.NTP. 129.70.130.70   2  u  5    64   357   68.795 -68.168 104.612
+europium.canoni 193.79.237.14   2  u  63   64   337   81.534 -67.968  92.792
```

و. مصادر

- راجع صفحة الويكي «Ubuntu Time» لمزيد من المعلومات.
- موقع ntp.org: الموقع الرسمي لمشروع بروتوكول وقت الشبكة.



ربط الأجهزة متعدد الطرق

ا. مقدمة عن DM-Multipath

يسمح لك «ربط الأجهزة بطرقٍ متعددة» (Device mapper multipathing [DM-Multipath]) بضبط طرق متعددة للدخل والخرج (I/O) بين عقد الخادوم ومصفوفات التخزين في جهاز واحد. طرق الدخل والخرج تلك هي اتصالات SAN فيزيائية التي تتضمن أكبالًا منفصلةً ومبدلات (switches) ومتحكمات (controllers)؛ يُجَمِّع تعددُ الطرقِ (multipathing) طرقَ الدخل والخرج، ويُنشِئ جهازًا جديدًا يحتوي على طرق مجمَّعة؛ يوفّر هذا الفصل ملخصًا عن ميزات DM-Multipath الجديدة لنسخة الخادوم ١٢.٠٤ من أوبنتو؛ وبعد ذلك سيوفر الفصل نظرة «عالية المستوى» عن DM-Multipath ومكوناته، ولمحة عن إعداده.

الميزات الجديدة والمعدلة لنسخة خادوم أوبنتو ١٢.٠٤

الانتقال من multipath-0.4.8 إلى multipath-0.4.9.

ا. الانتقال من ٠.٤.٨

لم تعد تعمل المتحققات من الأولوية كملفات ثنائية بحد ذاتها، بل كمكتبات مشتركة؛ وعُدِّل أيضًا اسم قيمة المفتاح (key) لهذه الميزة تعديلًا طفيفًا، انسخ الخاصية المسماة prio_callout إلى prio، وعدِّل الوسيط الممرر إلى المتحقق من الأولوية، حيث لم يعد يهم تمرير مسار النظام؛ مثال عن التحويل:

```
device {
          vendor "NEC"
          product "DISK ARRAY"
          prio_callout mpath_prio_alua /dev/%n
          prio      alua
}
```

راجع الجدول الآتي (التحويلات في متحقق الأولوية) لتفاصيل كاملة:

الجدول ٥-١: التحويلات في متحقق الأولوية

الإصدار ٠.٤.٨	الإصدار ٠.٤.٩
prio_callout mpath_prio_emc /dev/%n	prio emc
prio_callout mpath_prio_alua /dev/%n	prio alua
prio_callout mpath_prio_netapp /dev/%n	prio netapp
prio_callout mpath_prio_rdac /dev/%n	prio rdac
prio_callout mpath_prio_hp_sw /dev/%n	prio hp_sw
prio_callout mpath_prio_hds_modular %b	prio hds

ولما كان ملف الضبط الخاص بتعدد الطرق يُفسِّر جميع ثنائيات «المفتاح/القيمة» ويرى إن كان يستطيع استخدامهم، فيمكن أن يبقى كلٌ من prio_callout و prio معًا، لكن من المستحسن أن تُضاف الخاصية prio قبل بداية عملية الانتقال للإصدار الأحدث، ثم يمكنك أن تحذف الخاصية prio_callout القديمة بأمان، دون أن تسبب انقطاعًا في الخدمة.

يمكن أن يُستخدَم DM-Multipath لتوفير:

- Redundancy: يمكن أن يستخدم DM-Multipath في تجاوز فشل الأجهزة في حالة ضبط «فعال/غير فعال» (active/passive)؛ فيُستخدَم -في الضبط السابق- نصف عدد الطرق في آن واحد للدخل أو الخرج، وإذا فشل مكون من مكونات طريق الدخل أو الخرج (الكبل، أو المبدل، أو المتحكم)، فسيتحول DM-Multipath إلى طريق آخر بديل.

- تحسين الأداء: يمكن ضبط DM-Multipath للعمل في نمط «فعال/فعال» (active/active)، حيث يوزع الدخل أو الخرج بين الطرق عبر آلية round-robin، وفي بعض الإعدادات، يمكن أن يستشعر DM-Multipath الحِمل على طرق الدخل أو الخرج، ويعيد توازن الحمل ديناميكيًّا.

ب. لمحة عن مصفوفة التخزين

يتضمن DM-Multipath -افتراضيًا- دعمًا لأكثر مصفوفات التخزين شيوعًا التي تدعم DM-Multipath، الأجهزة المدعومة موجودة في ملف multipath.conf.defaults؛ إذا كانت مصفوفة التخزين الخاصة بك تدعم DM-Multipath، لكنها غير مضبوطة افتراضيًا في هذا الملف، فربما تحتاج لإضافتها إلى ملف ضبط DM-Multipath (multipath.conf)، للمزيد من المعلومات، راجع القسم «ملف ضبط DM-Multipath». تتطلب بعض مصفوفات التخزين تعاملًا خاصًا مع أخطاء الدخل أو الخرج، وتبديل الطرق؛ وهذا ما يتطلب وحداتٍ منفصلةً للنواة لدعم المتحكم العتادي.

ج. مكونات DM-Multipath

الجدول الآتي يشرح مكونات حزمة DM-Multipath:

الجدول ٥-١: مكونات DM-Multipath

المكون	الوصف
وحدة النواة dm_multipath	إعادة توجيه الدخل أو الخرج، ودعم تجاوز الفشل للطرق، ولمجموعات الطرق.
الأمر multipath	يعرض ويضبط أجهزة multipath، ويبدأ عمومًا مع /etc/rc.sysinit، ويمكن أن يشغَّل باستخدام برنامج udev عندما يضاف جهاز كتلي (block device) أو يمكن أن يشغَّل بواسطة initramfs.
عفريت multipathd	يراقب الطرق، وعندما يفشل طريقٌ ما ثم يعود إلى العمل، فإنه يهيّء مبدلات مجموعة الطريق؛ ويوفر تعديلات تفاعلية لأجهزة multipath؛ ويجب إعادة تشغيل هذا العفريت عندما تحدث أيّة تعديلات في ملف /etc/multipath.conf لكي تأخذ مفعولها.
الأمر kpartx	يُنشِئ أجهزة ربط الأجهزة (device mapper devices) للأقسام في الجهاز. من الضروري استخدام هذا الأمر للأقسام المبنية على DOS مع DM-Multipath، يُوفَّر الأمر kpartx في حزمة خاصة به، لكن الحزمة multipath-tools تعتمد عليه.

د. لمحة عن ضبط DM-Multipath

يحتـوي DM-Multipath علـى خيـارات افتراضـية مضـمَّنة بـه تلائـم أغلبيـة إعـدادات multipath؛ وتكـون عـادةً عمليـة إعـداد DM-Multipath عمليـةً بسـيطةً، فالعمليـة الأساسـية لضبط نظامك مع DM-Multipath هي كالآتي:

١. تثبيت حزمتَي multipath-tools، و multipath-tools-boot.

٢. إنشاء ملف ضبط فارغ /etc/multipath.conf، الذي سيعيد تعريف ما سيلي ذكره لاحقًا.

٣. إذا كان ذلك ضروريًا، حرِّر ملف ضبط multipath.conf لتعديل القيم الافتراضية، ثم احفظ الملف المعدَّل.

٤. ابدأ عفريت multipath.

٥. حدِّث «initial-ramdisk».

لخطوات إعداد مفصلة لضبط multipath، راجع القسم «إعداد DM-Multipath».

٢. أجهزة Multipath

سيعامل كل طريق من عقدة الخادوم إلى متحكم التخزين كجهاز منفصل إذا لم تستعمل DM-Multipath، حتى لو كان طريق الدخل أو الخرج يصل نفس عقدة الخادوم بنفس متحكم التخزين، حيث يوفر DM-Multipath طريقةً لتنظيم طرق الدخل أو الخرج منطقيًا، وذلك بإنشاء جهاز multipath وحيد فوق عدة أجهزة تمثل طبقةً تحتيةً.

ا. معرفات الجهاز متعدد الطرق

لكل جهاز متعدد الطرق (multipath device) معرف عالمي (WWID)، الذي يضمن أن يكون فريدًا عالميًا، ولا يمكن تعديله؛ يُضبَط اسم جهاز multipath افتراضيًا إلى WWID الخاص به؛ لكن يمكنك ضبط خيار user_friendly_names في ملف إعدادات multipath الذي يجعل DM-Multipath يستخدم أسماءً بديلة فريدة لكل عقدة من الشكل mpathn.

على سبيل المثال، إذا كانت عقدةٌ ما ذات جهازَي HBA موصولةً إلى متحكم تخزين بمنفذين عبر مبدل FC غير مُقسَّمٍ لمناطق، فإنه يرى أربعة أجهزة: /dev/sda/، و /dev/dsb/، و /dev/sdb/، و /dev/sdd/. يُنشِئ DM-Multipath جهازًا وحيدًا بعنوان WWID فريد الذي يعيد توجيه الدخل أو الخرج لهذه الأجهزة الأربعة وفقًا لضبط multipath، وعندما يفعَّل خيار الضبط user_friendly_names، فسيُضبَط اسم الجهاز إلى mapthn، حيث ستُشاهَد الأجهزة الجديدة التي توضع تحت سيطرة DM-Multipath في مكانين مختلفَين في مجلد /dev هما: /dev/mapper/mpathn/، و /dev/dm-n/.

تُنشَأ الأجهزة في /dev/mapper في مرحلة مبكرة من عملية الإقلاع، استخدم هذه الأجهزة للوصول إلى الأجهزة المتعددة الطرق، على سبيل المثال عند إنشاء الحجوم المنطقية (logical volumes). أيّة أجهزة من النمط /dev/dm-n تُستخدَم داخليًا فقط، ولا يجب أن تُستعمَل من مدير النظام أبدًا.

للمزيد من المعلومات حول ضبط multipath الافتراضي، بما في ذلك خيار الضبط user_friendly_names، راجع القسم «الإعدادات الافتراضية لملف الضبط»؛ يمكنك ضبط اسم جهاز multipath إلى اسم من اختيارك باستخدام الخيار alias في قسم multipaths في ملف ضبط multipath؛ للمزيد من المعلومات حول قسم multipaths في ملف ضبط multipath، راجع القسم «خاصيات ملف ضبط Multipath».

ب. اتساق أسماء أجهزة Multipath في شبكة عنقوديّة

عندما يكون خيار الضبط user_friendly_names مضبوطًا إلى «yes»، فإن اسم جهاز multipath هو فريد بالنسبة للعقدة، لكن ليس مضمونًا أن يكون هو نفسه في جميع العقد التي تستخدم جهاز multipath. وبشكل مشابه، إذا استخدمت الخيار alias للجهاز في قسم multipaths في ملف الضبط multipath.conf، فإن الاسم لن يكون ذاته متناسقًا تلقائيًا في جميع العقد في الشبكة العنقودية. هذا لن يؤدي إلى حدوث صعوبات إذا كنت تستخدم LVM لإنشاء أجهزة منطقية من جهاز العقدة. لكن إن كنت تتطلب أن تكون أسماء جميع أجهزة multipath في كل عقدة متناغمةً، فإنه من المستحسن أن تترك الخيار user_friendly_names مضبوطًا إلى «no»، وألّا تضبط أسماءً بديلةً لأجهزتك.

وبشكل مشابه، إذا أردت ضبط اسم بديل للجهاز، لكنك تريده أن يكون متناسقًا في جميع العقد في الشبكة العنقودية، فعليك أن تتأكد أن الملف /etc/multipath.conf هو نفسه في كل عقدة في الشبكة العنقودية، باستخدام هذه الطريقة:

- اضبط الأسماء البديلة لأجهزة multipath في ملف multipath.conf في حاسوب واحد.
- عطل جميع أجهزة multipath في حواسيبك البقية بتطبيق الأوامر الآتية:

```
sudo service multipath-tools stop
sudo multipath -F
```

- انسخ ملف multipath.conf من الجهاز الأول إلى جميع الأجهزة البقية في الشبكة العنقودية.
- أعد تفعيل عفريت multipathd في جميع الأجهزة الأخرى في الشبكة العنقودية بتطبيق الأمر الآتي:

```
sudo service multipath-tools start
```

عليك إعادة تنفيذ هذه العملية عند كل إضافة لجهاز جديد.

ج. خواص جهاز Multipath

بالإضافة لخيارَيّ user_friendly_names و alias، لدى جهاز multipath خاصياتٌ عديدة؛ تستطيع تعديل هذه الخاصيات لجهاز multipath معين بإنشاء مدخلة (entry) لذاك الجهاز في قسم multipaths في ملف إعدادات multipath. لمزيد من المعلومات حول قسم multipaths في ملف إعدادات multipath، راجع القسم «خاصيات ملف ضبط Multipath».

د. أجهزة multipath في الحجوم المنطقية

بعد إنشاء أجهزة multipath، يمكنك استخدام أسماء أجهزة multipath كما لو كنت تستخدم اسم جهاز فيزيائي عندما تُنشِئ حجمًا فيزيائيًا في LVM؛ على سبيل المثال، إذا كان /dev/mapper/mpatha هو اسم جهاز multipath، فإن الأمر الآتي سيُعَلِّم /dev/mapper/mpatha كحجم فيزيائي:

```
sudo pvcreate /dev/mapper/mpatha
```

يمكنك استخدام جهاز LVM الفيزيائي الناتج لإنشاء مجموعة حجوم LVM كما لو كنت تستخدم أي جهاز LVM فيزيائي آخر.

ملاحظة: لو كنت تحاول إنشاء حجم LVM فيزيائي على كامل الجهاز الذي ضبطت عليه أقسامًا، فسيفشل تنفيذ الأمر pvcreate.

عندما تُنشِئ حجم LVM منطقي، الذي يستخدم مصفوفات multipath «فعال/غير فعال» كبنية تحتية للأجهزة الفيزيائية؛ فعليك تضمين مرشحات (filters) في ملف lvm.conf لاستثناء هذه الأقراص التي تكوّن البنية التحتية لأجهزة multipath؛ وهذا لأنه لو كانت المصفوفة تغير تلقائيًا الطريق الفعال إلى طريق غير فعال عندما تتلقى دخلًا أو خرجًا، فإن multipath سيتجاوز الفشل، لكنه «سيفشل» عندما يتفحص LVM الطريق غير الفعال إذا لم تُرشَّح تلك الأجهزة، سيعرض LVM رسالة تحذير عندما يحدث ذلك في مصفوفات «فعال/غير فعال» (التي تتطلب أمرًا لجعل الطريق غير الفعال فعالًا). لترشيح جميع أجهزة SCSI في ملف ضبط LVM ‏(lvm.conf)، فضع المرشح الآتي في قسم الأجهزة في الملف:

```
filter = [ "r/block/", "r/disk/", "r/sd.*/", "a/.*/" ]
```

من الضروري بعد تحديث ملف /etc/lvm.conf أن يُحدَّث initrd لذلك سيُنسَخ هذا الملف هناك، حيث يهم المرشح كثيرًا أثناء الإقلاع؛ نفذ الأمر:

```
update-initramfs -u -k all
```

ملاحظة: في كل مرة يُحدَّث فيها ملف /etc/lvm.conf أو /etc/multipath.conf، فيجب إعادة بناء initrd لتطبيق هذه التغيرات، هذا الأمر واجبٌ عندما تكون القوائم السوداء والمرشحات ضروريةً للحفاظ على ضبطٍ للتخزين ذي بنيةٍ صلبةٍ.

٣. لمحة عن ضبط DM-Multipath

يوفر هذا القسم مثالًا لخطوات ضبط DM-Multipath، حيث يتضمن الخطوات الآتية:

- إعداد DM-Multipath أساسي.
- تجاهل الأقراص المحلية.
- إضافة المزيد من الأجهزة إلى ملف الإعدادات.

ا. إعداد DM-Multipath

قبل إعداد DM-Multipath على نظامك، تأكد أن نظامك محدَّث ويتضمن الحزمة multipath-tools؛ إذا كان المطلوب هو الإقلاع من SAN، فيجب أيضًا أن تتوفر الحزمة multipath-tools-boot.

لا يُشترَط أن يتوفر ملف /etc/multipath.conf، فعندما يُشغَّل multipath دون وجود ملف /etc/multipath.conf، فإنه يستخدم قاعدة بيانات داخلية لإيجاد ضبط ملائم، ويستعمل أيضًا القائمة السوداء الداخلية، وإذا لم تُكتَشف أيّة طرق بعد تشغيل multipath -ll، فيجب توفير طريق لزيادة درجة الإسهاب لاكتشاف لماذا لم يُنشَأ multipath. خذ بعين الاعتبار الرجوع إلى توثيق شركة SAN؛ توجد أمثلة عن ملفات الضبط في /usr/share/doc/multipath-tools/examples، وقاعدة بيانات multipathd حية:

```
# echo 'show config' | multipathd -k > multipath.conf-live
```

ملاحظة: لتجاوز حالة خاصة في multipathd عندما لا يتوفر ملف etc/multipath.conf/، عندئذٍ لا يعيد الأمر السابق أيّة مخرجات كنتيجةٍ لعملية الدمج بين etc/multipath.conf/ وقاعدة البيانات في الذاكرة؛ فلحل ذلك، إما أن تعرِّف ملف etc/multipath.conf/ فارغ باستخدام الأمر touch؛ أو أن تعيد تعريف القيمة الافتراضية كما يلي:

```
defaults {
	user_friendly_names no
}
```

وأعد تشغيل multipathd:

```
sudo service multipath-tools restart
```

سيعيد الأمر «show config» قاعدة البيانات الحية.

التثبيت مع دعم Multipath

لتفعيل دعم multipath أثناء التثبيت، استخدم:

```
install disk-detect/multipath/enable=true
```

في مِحَث المثبت؛ وستظهر أثناء التثبيت أجهزة multipath المُكتشَفة في:

```
/dev/mapper/mpath<X>
```

ب. تجاهل الأقراص المحلية أثناء توليد أجهزة Multipath

لبعض الحواسيب بطاقات SCSI لأقراصها المحلية؛ وليس من المستحسن استخدام DM-Multipath لهذه الأقراص، ستظهر العملية الآتية كيفية تعديل ملف ضبط multipath لتجاهل الأقراص المحلية أثناء ضبط multipath.

حدد أيّة أقراص هي الأقراص الداخلية، وعلّمها كتلك الموجودة في القائمة السوداء؛ إن /dev/sda -في هذا المثال- هو قرص داخلي، لاحظ أنه مضبوط أصليًا في ملف ضبط multipath الافتراضي، سيُظهِر الأمر multipath -v2 القرص المحلي (/dev/sda) في خريطة multipath؛ للمزيد من المعلومات حول ناتج خرج الأمر multipath، راجع القسم «ناتج الأمر multipath».

```
sudo multipath -v2
   create: SIBM-ESXSST336732LC____F3ET0EP0Q000072428BX1 undef
WINSYS,SF2372
   size=33 GB features="0" hwhandler="0" wp=undef
   `-+- policy='round-robin 0' prio=1 status=undef
      |- 0:0:0:0 sda 8:0 [---------

   device-mapper ioctl cmd 9 failed: Invalid argument
   device-mapper ioctl cmd 14 failed: No such device or address
   create: 3600a0b80001327d80000006d43621677 undef
WINSYS,SF2372
   size=12G features='0' hwhandler='0' wp=undef
   `-+- policy='round-robin 0' prio=1 status=undef
      |- 2:0:0:0 sdb 8:16 undef ready running
        `- 3:0:0:0 sdf 8:80 undef ready         running

   create: 3600a0b80001327510000009a436215ec undef
WINSYS,SF2372
   size=12G features='0' hwhandler='0' wp=undef
   `-+- policy='round-robin 0' prio=1 status=undef
      |- 2:0:0:1 sdc 8:32 undef ready         running
        `- 3:0:0:1 sdg 8:96 undef ready         running

   create: 3600a0b80001327d800000070436216b3 undef
WINSYS,SF2372
   size=12G features='0' hwhandler='0' wp=undef
   `-+- policy='round-robin 0' prio=1 status=undef
      |- 2:0:0:2 sdd 8:48 undef ready         running
        `- 3:0:0:2 sdg 8:112 undef ready         running
```

```
   create: 3600a0b800013275100000009b4362163e undef
WINSYS,SF2372
   size=12G features='0' hwhandler='0' wp=undef
   `-+- policy='round-robin 0' prio=1 status=undef
      |- 2:0:0:3 sdd 8:64 undef ready running
        `- 3:0:0:3 sdg 8:128 undef ready running
```

لكي يُمنَع رابط الأجهزة من ربط /dev/sda في خرائط multipath الخاصة به، فعدِّل قسم القائمة السوداء (blacklist) في ملف /etc/multipath.conf لتضمين هذا الجهاز، على الرغم من أنك تستطيع جعل الجهاز sda ضمن القائمة السوداء باستخدام النوع devnode، لكنها لن تكون طريقةً آمنةً لأننا لا يمكن أن نضمن أن /dev/sda سيبقى بنفس الاسم عند إعادة التشغيل؛ لإضافة أجهزة منفصلة إلى القائمة السوداء، فيمكنك استخدام WWID لذاك الجهاز، لاحظ أنه قد ظهر في مخرجات الأمر multipath -v2 مُعرِّف WWID للجهاز /dev/sda وكان SIBM-ESXSST336732LC____F3ET0EP0Q000072428BX1؛ أضف ما يلي في ملف /etc/multipath.conf لحجبه:

```
blacklist {
          wwid SIBM-ESXSST336732LC____F3ET0EP0Q000072428BX1
}
```

بعد أن تُحدِّث ملف /etc/multipath.conf، يجب أن تخبر multipathd يدويًا أن يُعيد قراءة الملف، يعيد الأمر الآتي قراءة ملف /etc/multipath.conf المُعدَّل:

```
sudo service multipath-tools reload
```

نفذ الأمر الآتي لإزالة جهاز multipath:

```
sudo multipath -f SIBM-ESXSST336732LC____F3ET0EP0Q000072428BX1
```

للتحقق فيما إذا نجحت عملية إزالة الجهاز، يمكنك تنفيذ الأمر multipath -ll لعرض ضبط multipath الحالي، راجع القسم «طلبيات Multipath باستخدام الأمر multipath» للمزيد من المعلومات حول الأمر multipath -ll. للتأكد من أن الجهاز المضاف إلى القائمة السوداء لم يُضَف مرةً ثانيةً، فتستطيع تنفيذ الأمر multipath كما في المثال الآتي؛ حيث يُضبَط الأمر multipath افتراضيًا بأن يجعل درجة «الإسهاب» (verbosity) من الدرجة v2 إذا لم تُحدِّد الخيار -v:

```
   sudo multipath

   create: 3600a0b80001327d80000006d43621677 undef
WINSYS,SF2372
   size=12G features='0' hwhandler='0' wp=undef
   `-+- policy='round-robin 0' prio=1 status=undef
      |- 2:0:0:0 sdb 8:16       undef ready     running
        `- 3:0:0:0 sdf 8:80 undef ready          running

   create: 3600a0b80001327510000009a436215ec undef
WINSYS,SF2372
   size=12G features='0' hwhandler='0' wp=undef
   `-+- policy='round-robin 0' prio=1 status=undef
      |- 2:0:0:1 sdc 8:32 undef ready running
        `- 3:0:0:1 sdg 8:96 undef ready running

   create: 3600a0b80001327d800000070436216b3 undef
WINSYS,SF2372
   size=12G features='0' hwhandler='0' wp=undef
   `-+- policy='round-robin 0' prio=1 status=undef
      |- 2:0:0:2 sdd 8:48 undef ready          running
        `- 3:0:0:2 sdg 8:112 undef ready          running
```

```
   create: 3600a0b800013275100000009b4362163e undef
WINSYS,SF2372
   size=12G features='0' hwhandler='0' wp=undef
   `-+- policy='round-robin 0' prio=1 status=undef
      |- 2:0:0:3 sdd 8:64 undef ready          running
        `- 3:0:0:3 sdg 8:128 undef ready          running
```

ج. ضبط أجهزة التخزين

يتضمن DM-Multipath افتراضيًا دعمًا لأغلبية مصفوفات التخزين التي تدعم DM-Multipath، قيم الإعدادات الافتراضية، بما فيها الأجهزة المدعومة، يمكن أن توجد في ملف multipath.conf.defaults.

إذا احتجت لإضافة جهاز تخزين غير مدعوم افتراضيًا كجهاز multipath معروف، فعدل ملف /etc/multipath.conf وأضف معلومات الجهاز الملائمة.

على سبيل المثال، لإضافة معلومات حول سلسلة HP Open-V، فستبدو المدخلة كما يلي، حيث n% هو اسم الجهاز:

```
devices {
      device {
              vendor "HP"
              product "OPEN-V."
              getuid_callout "/lib/udev/scsi_id --whitelisted
--device=/dev/%n"
      }
}
```

للمزيد من المعلومات حول قسم الأجهزة في ملف الضبط، انظر قسم «ملف ضبط الأجهزة».

٤. ملف ضبط DM-Multipath

تستطيع تجاوز قيم ضبط DM-Multipath الافتراضية بتعديل ملف الضبط /etc/multipath.conf؛ ويمكنك إضافة مصفوفات التخزين غير المدعومة افتراضيًا في ملف الإعدادات إن كان ذلك ضروريًا؛ يوفر هذا الفصل معلوماتٍ عن تفسير وتعديل ملف multipath.conf، ويحتوي أقسامًا عن المواضيع الآتية:

- لمحة عن ملف الضبط.
- ملف ضبط القائمة السوداء.
- ملف ضبط القيم الافتراضية.
- ملف ضبط خاصيات Multipath.
- ملف ضبط الأجهزة.

ستحتاج -في ملف ضبط multipath- إلى تحديد الأقسام التي تحتاج لها للضبط الذي تريده، أو إذا أردت تغيير القيم الافتراضية المضبوطة في ملف multipath.conf.defaults؛ إذا كانت هنالك أقسام ليست متعلقة ببيئة عملك، أو التي لا تحتاج إلى تجاوز قيمها الافتراضية، فإنك تستطيع أن تتركها وقبلها رمز التعليق، كما كانت في الملف الابتدائي.

يسمح لك ملف الضبط باستخدام التعابير النمطية.

يمكن العثور على نسخةٍ مليئةٍ بالتعلقيات من مثالٍ عن ملف الإعدادات في المسار:

```
/usr/share/doc/multipath-tools/examples/multipath.conf.annotated.gz
```

أ. لمحة عن ملف الضبط

يُقسّم ملف ضبط multipath إلى الأقسام الآتية:

- blacklist: قائمة بالأجهزة التي لا تدخل بعين الاعتبار عند استخدام multipath.
- blacklist_exceptions: قائمة بالأجهزة المرشحة لتكون جزءًا من multipath التي كان يجب أن تكون في القائمة السوداء، وذلك وفقًا لضبط قسم القائمة السوداء.
- defaults: إعدادات DM-Multipath افتراضية عامة.
- multipath: إعدادات لصفات أجهزة multipath الفردية، ستتجاوز هذه القيم ما هو محدد في قسمَيّ defaults و devices من ملف الضبط.
- devices: الإعدادات لكل متحكم من متحكمات التخزين، هذه القيم ستتجاوز تلك المحددة في قسم defaults في ملف الضبط، إذا كنت تستخدم مصفوفة تخزين ليست مدعومة افتراضيًا، فربما تحتاج لإنشاء قسم فرعي من devices لمصفوفتك.

عندما يُحدِّد النظام خاصيات جهاز multipath، فإنه يتحقق أولًا من إعدادات multipath، ثم إعدادات كل جهاز على حدة، ثم القيم الافتراضية لنظام multipath.

ب. ملف ضبط القائمة السوداء

قسم القائمة السوداء من ملف ضبط multipath يحدد الأجهزة التي لن تستخدم عندما يضبط النظام أجهزة multipath، الأجهزة الموجودة في القائمة السوداء لن تجمَّع إلى جهاز multipath.

إذا أردت حجب الأجهزة، فيمكنك فعل ذلك عبر أحد الشروط الآتية:

- بواسطة معرف WWID، كما هو مشروحٌ في قسم «الحجب بواسطة WWID».
- بواسطة اسم الجهاز، كما هو مشروحٌ في قسم «الحجب بواسطة اسم الجهاز».
- بواسطة نوع الجهاز، كما هو مشروحٌ في قسم «الحجب بواسطة نوع الجهاز».

هنالك مختلف أنواع الأجهزة المُضَافة إلى القائمة السوداء افتراضيًا حتى لو عطّلتَ القسم الابتدائي للقائمة السوداء في ملف الضبط، لمعلوماتٍ حول ذلك، راجع قسم «الحجب بواسطة اسم الجهاز».

الحجب بواسطة WWID

يمكنك إضافة أجهزة معينة إلى القائمة السوداء بواسطة معرفها العالمي باستخدام القيد wwid في قسم blacklist في ملف الضبط.

يُظهِر المثال الآتي الأسطر في ملف الضبط التي ستحجب جهازًا معرِّفه العالمي هو 26353900f02796769:

```
blacklist {
        wwid 26353900f02796769
}
```

الحجب بواسطة اسم الجهاز

تستطيع حجب أنواع الأجهزة عبر اسم الجهاز، مما يؤدي إلى عدم جمعها في جهاز multipath بتحديد القيد devnode في قسم blacklist من ملف الضبط.

يوضح المثال الآتي الأسطر في ملف الضبط التي تستخدم لحجب جميع أجهزة SCSI، حيث أنها تحجب كل أجهزة *sd:

```
blacklist {
          devnode "^sd[a-z]"
}
```

تستطيع استخدام القيد devnode في قسم blacklist في ملف الضبط لتحديد الأجهزة كلًّا على حدة بدلًا من تحديد جميع الأجهزة من نوع معيّن، لكن هذا ليس مستحسنًا، لأنها إن لم تكن هذه الأجهزة معرَّفة ومربوطة ربطًا ثابتًا باستخدام قواعد udev، فليس هنالك أيّة ضمانة أن الجهاز المحدد سيكون له نفس الاسم بعد إعادة الإقلاع؛ فعلى سبيل المثال، ربما يتغير اسم الجهاز من dev/sda/ إلى dev/sdb/ عند إعادة الإقلاع.

قيود devnode الآتية موجودة في القائمة السوداء افتراضيًا؛ الأجهزة التي تحجبها هذه القيود لا تدعم DM-Multipath عمومًا، ولتفعيل تعدد الطرق في أي جهاز من تلك الأجهزة، فعليك تحديده في قسم blacklist_exceptions في ملف الضبط، كما هو موضح في قسم «استثناءات الحجب»:

```
blacklist {
         devnode "^(ram|raw|loop|fd|md|dm-|sr|scd|st)[0-9]*"
         devnode "^hd[a-z]"
}
```

الحجب بواسطة نوع الجهاز

تستطيع تحديد أنواع أجهزة معينة في قسم blacklist من ملف الضبط باستخدام قسم device، المثال الآتي يحجب كل أجهزة IBM DS4200 وأجهزة HP.

```
blacklist {
        device {
                vendor   "IBM"
                product  "3S42"       #DS4200 Product 10
        }
        device {
                vendor   "HP"
                product  "*"
        }
}
```

استثناءات الحجب

تستطيع استخدام قسم blacklist_exceptions في ملف الضبط لتفعيل تعدد الطرق في الأجهزة المحجوبة افتراضيًا.

على سبيل المثال، إذا كان لديك عددٌ كبيرٌ من الأجهزة، وتريد أن تسمح لجهاز واحد فقط أن يدخل في multipath (ويكون WWID الخاص به هو 3600d0230000000000e13955cc3757803)، فبدلًا من حجب كل الأجهزة يدويًا ما عدا الجهاز الذي تريد استخدامه، فيمكنك حجب جميع الأجهزة، وتسمح لذاك الجهاز الوحيد أن يعمل بإضافة الأسطر الآتية إلى ملف /etc/multipath.conf:

```
blacklist {
         wwid "*"
}

blacklist_exceptions {
         wwid "3600d0230000000000e13955cc3757803"
}
```

عند تحديد الأجهزة المسموحُ لها في قسم blacklist_exceptions من ملف الضبط، فعليك تحديد تلك الاستثناءات بنفس الطريقة التي حددت فيها الأجهزة المحجوبة في قسم blacklist؛ فعلى سبيل المثال، لا يمكن السماح لجهاز بوساطة معرف WWID في حال حجبت الأجهزة باستخدام قيد devnode، حتى لو كان الجهاز المحجوب مرتبطًا بمعرف WWID الذي حددَته أنت. وبشكل مشابه، الاستثناءات التي تستخدم devnode تُطبَّق فقط على قيود devnode، وكذلك الأمر لاستثناءات الأجهزة.

ج. الإعدادات الافتراضية لملف الضبط

يتضمن ملف الضبط /etc/multipath.conf قسمًا اسمه defaults يضبط خاصية user_friendly_names إلى القيمة yes، كما يلي:

```
defaults {
          user_friendly_names yes
}
```

وهذا يتجاوز القيمة الافتراضية لخاصية user_friendly_names.

ويحتوي ملف الضبط قالبًا للإعدادات الافتراضية للضبط، هذا القسم معطل بالتعليقات كما يلي:

```
#defaults {
#         udev_dir                /dev
#         polling_interval        5
#         selector                "round-robin 0"
#         path_grouping_policy failover
#         getuid_callout          "/lib/dev/scsi_id --whitelisted
--device=/dev/%n"
# prio   const
# path_checker   directio
# rr_min_io   1000
# rr_weight   uniform
# failback   manual
# no_path_retry   fail
# user_friendly_names   no
#}
```

لتجاوز قيمة افتراضية في أيّة خاصية من خاصيات الضبط، تستطيع نسخ السطر الموافق لها من القالب إلى قسم defaults وإزالة التعليق الذي قبلها؛ على سبيل المثال، لتجاوز الخاصية path_grouping_policy لتضبَط إلى القيمة multibus بدلًا من failover؛ فانسخ ذاك السطر من القالب إلى قسم defaults الابتدائي من ملف الضبط، ثم أزل التعليق كما يلي:

```
defaults {
          user_friendly_names        yes
          path_grouping_policy       multibus
}
```

يشرح الجدول الآتي الخاصيات التي يمكنك ضبطها في قسم defaults من ملف multipath.conf، ستُستخدَم هذه القيم من DM-Multipath ما لم يعاد تعريفها باستخدام الخصائص المحددة في قسمَيّ devices و multipaths في ملف multipath.conf.

الجدول ٥-٣: القيم الافتراضية لملف ضبط Multipath

الخاصية	الشرح
polling_interval	تحديد الزمن الفاصل بين التحققين من الطرق بالثواني، سيزداد الزمن الفاصل للتحقق من الطرق التي تعمل عملًا سليمًا تدريجيًا إلى (٤ * polling_interval)، القيمة الافتراضية هي ٥.
udev_dir	المجلد الذي تُنشأ فيه عقد أجهزة udev، القيمة الافتراضية هي dev/.
multipath_dir	المجلد الذي تُخزَّن فيه الكائنات المشتركة الديناميكية، القيمة الافتراضية متعلقةٌ بنظام التشغيل، وتكون عادةً القيمة lib/multipath/.
verbosity	قيمة «الإسهاب» الافتراضية. تزيد القيم العليا من درجة الإسهاب، وتتراوح القيم الصالحة بين ٠ و ٦، القيمة الافتراضية هي ٢.
path_selector	توصيف الخوارزمية الافتراضية لتحديد أي طريق سيستخدم في عملية الدخل أو الخرج الآتية، القيم الممكنة تتضمن: • round-robin 0: المرور على كل طريق في مجموعة الطرق، وإرسال نفس كمية الدخل أو الخرج لكلٍ منها. • queue-length 0: إرسال رزمة الدخل أو الخرج الآتية في الطريق الذي يحتوي على أقل عدد من طلبيات الدخل أو الخرج. • service-time 0: يرسل رزمة الدخل أو الخرج الآتية في الطريق الذي يكون له وقت خدمة أقصر ما يمكن، وهذا يُحدَّد بتقسيم حجم رزم الدخل أو الخرج التي ما زالت في كل طريق على وقت مرورها (النسبي). القيمة الافتراضية هي round-robin 0.

path_grouping_policy	تحديد الطريق الافتراضي لسياسة تجميع الطرق لتطبَّق على الطرق المتعددة غير المحددة؛ القيم الممكنة هي: • القيمة failover: طريق وحيدٌ لكل مجموعة أولويات. • القيمة multibus: جميع الطرق الصالحة في مجموعة أولويات واحدة. • القيمة group_by_serial: مجموعة أولويات وحيدة لكل رقم تسلسلي كُشِفَ عنه. • القيمة group_by_prio : مجموعة أولويات وحيدة لكل طريق حسب قيمة أولويته. • القيمة group_by_node_name : مجموعة أولويات وحيدة لكل اسم عقدة هدف. القيمة الافتراضية هي failover.
getuid_callout	تحديد البرنامج الافتراضي ووسائطه الممررة إليه الذي يجب استدعاؤه للحصول على معرِّفٍ فريدٍ للطريق؛ يجب تحديد مسار مطلق له. القيمة الافتراضية هي: /lib/udev/scsi_id --whitelisted --device=/dev/%n

prio	تحديد الدالة الافتراضية لاستدعائها للحصول على قيمة أولوية الطريق، على سبيل المثال، بتات ALUA في SPC-3 توفر قيمة prio يمكن الاستفادة منها. القيم الممكنة هي: • القيمة const: تحديد الأولوية ١ إلى جميع الطرق. • القيمة emc: توليد أولوية الطريق لمصفوفات EMC. • القيمة alua: توليد أولوية الطريق بالاعتماد على إعدادات SCSI-3 ALUA. • القيمة netapp: توليد أولوية الطريق لمصفوفات NetApp. • القيمة rdac: توليد أولوية الطريق لمتحكم LSI/Engenio RDAC. • القيمة hp_sw: توليد أولوية الطريق لمتحكم Compaq/HP في نمط «فعال/في وضع الاستعداد». • القيمة hds: توليد أولوية الطريق لمصفوفات تخزين Hitachi HDS. القيمة الافتراضية هي const.
prio_args	السلسلة النصية للوسائط الممررة إلى دالة prio؛ لا تحتاج أغلبية دوال prio إلى وسائط، لكن دالة «datacore prioritizer» تحتاج واحدًا، على سبيل المثال: «timeout=1000 preferredsds=foo»؛ القيمة الافتراضية هي لا شيء ("").
features	الخاصيات الإضافية لأجهزة multipath، الخاصية الوحيدة الموجودة هي queue_if_no_path، التي هي نفس الضبط no_path_retry إلى queue، للمزيد من المعلومات حول المشاكل التي ستحصل عند استخدام هذه الخاصية، راجع القسم «المشاكل مع queue_if_no_path».

path_checker	توصيف الطريقة الافتراضية المستخدمة لتحديد حالة الطرق، القيم الممكنة تتضمن: القيمة readsector0: قراءة القطاع الأول من الجهاز. القيمة tur: تنفيذ «TEST UNIT READY» على الجهاز. القيمة emc_clariion: طلب صفحة EVPD (التي هي 0xC0) من EMC Clariion لتحديد الطريق. القيمة hp_sw: التحقق من حالة الطريق لمصفوفات HP للتخزين التي تعمل بنمط «فعال/في وضع الاستعداد». القيمة rdac: التحقق من حالة الطريق لمتحكم التخزين LSI/Engenio RDAC. القيمة directio: قراءة أول قطاع باستخدام الدخل أو الخرج المباشر. القيمة الافتراضية هي directio.
failback	تدير آلية تجاوز الفشل في مجموعة الطرق. القيمة immediate تؤدي إلى تجاوز الفشل مباشرةً إلى مجموعة الطرق ذات أعلى أولوية وتحتوي على طرق فعالة. القيمة manual تشير إلى أنه لا يجب أن تكون هنالك آلية لتجاوز الفشل مباشرةً، ويتم ذلك بتدخل مسؤول النظام. قيمة رقمية أكبر من الصفر تحدد زمن التأجيل لتجاوز الفشل مُعبَّرًا عنه بالثواني. القيمة الافتراضية هي manual.
rr_min_io	تحدد عدد طلبيات الدخل أو الخرج لتمريرها إلى طريقٍ ما قبل الانتقال إلى الطريق الآتي في مجموعة الطرق الحالية. القيمة الافتراضية هي ١٠٠٠.

rr_weight	إذا ضُبِطَت إلى priorities فعندئذٍ بدلًا من إرسال طلبيات rr_min_io إلى طريقٍ ما قبل استدعاء path_selector لتحديد الطريق الآتي، فإنه يُحدَّد رقم الطلبيات التي ستُرسَل بواسطة جداء rr_min_io بأولوية الطريق، كما هو محدد بواسطة دالة prio. وإذا ضبطت الخاصية إلى uniform، فإن «ثقل» كل الطرق سيكون متساويًا. القيمة الافتراضية هي uniform.
no_path_retry	تُحدِّد القيمة العددية لهذه الخاصية عدد المرات التي سيحاول فيها النظام استخدام الطريق التي تعرض للفشل قبل إيقاف الطلبيات. إذا كانت القيمة «fail» فهذا يعني أن الفشل سيكون فوريًا دون أيّة طلبيات؛ وإذا كانت القيمة queue، فهذا يعني أنه لا يجب أن تتوقف الطلبيات حتى يصلَّح ذاك الطريق. القيمة الافتراضية هي "صفر".
user_friendly_ names	إذا ضبطت إلى yes، فإنها تحدد أن على النظام استخدام الملف /etc/multipath/bindings لتعيين اسم بديل فريد للطريق، على شكل mpathn؛ وإذا ضبطت إلى no، فإن على النظام استخدام WWID كاسم بديل للطريق؛ وفي كلا الحالتين، ما سيُحدَّد هنا سيتم تجاوزه من أيّة أسماء بديلة خاصة بالأجهزة محددة في قسم multipaths من ملف الضبط. القيمة الافتراضية هي no
queue_without _daemon	إذا ضبطت إلى no، فسيُعطِّل عفريت multipathd جميع الطلبيات لجميع الأجهزة عندما يكون مغلقًا. القيمة الافتراضية هي no.

flush_on_last_del	إذا ضبطت إلى yes، فإن multipath سيعطل الطلبيات عندما يحذف آخر طريق إلى جهازٍ ما. القيمة الافتراضية هي no.
max_fds	تضبط العدد الأقصى من مقابض الملفات المفتوحة (open file descriptors) التي يمكن أن تُفتَح بواسطة multipath وعفريت multipathd؛ وهذا مكافئ للأمر ulimit -n؛ القيمة القصوى ستُحدد إلى النظام من ملف /proc/sys/fs/nr_open، إذا لم تضبط هذه الخاصية، فإن الرقم الأقصى لمقابس الملفات المفتوحة سيأخذ من العملية المُستدعِيَة؛ الذي يكون عادة ١٠٢٤، ولكي تكون آمنًا، يجب ضبط الخاصية إلى العدد الأقصى من الطرق زائد ٣٢ إذا كان هذا الرقم أكبر من ١٠٢٤.
checker_timer	المهلة الممنوحة لمتحققي الطرق لتنفيذ أوامر SCSI بالثواني. القيمة الافتراضية مأخوذة من /sys/block/sdx/device/timeout التي هي ٣٠ ثانية في نسخة أوبنتو ١٢.٠٤.
fast_io_fail_tmo	عدد الثواني التي ستنتظرها طبقة SCSI بعد اكتشاف حدوث مشكلة في منفذ FC بَعيد قبل إعلان فشل الدخل أو الخرج إلى الأجهزة في ذاك المنفذ البعيد؛ يجب أن تكون هذه القيمة أصغر من قيمة dev_loss_tmo. ضبط هذه القيمة إلى off سيعطل المهلة. القيمة الافتراضية محددة من نظام التشغيل.
dev_loss_tmo	عدد الثواني التي ستنتظرها طبقة SCSI بعد اكتشاف حدوث مشكلة في منفذ FC بَعيد قبل إزالته من النظام؛ ضبط هذه القيمة إلى infinity ستجعل قيمته ٢١٤٧٤٨٣٦٤٧ ثانية، أو ٦٨ سنة. القيمة الافتراضية محددة من نظام التشغيل.

د. خواص ملف ضبط Multipath

جـدول خاصـيات Multipath الآتـي يوضـح الخاصـيات الـتي يمكـن أن تضـبط فـي قسـم multipaths في ملف multipath.conf لكل جهاز multipath محدد؛ ستطبق هذه الخاصيات على multipath وحيد محدد، ستُستخدَم هذه القيم الافتراضية من DM-Multipath وستتجاوز الخاصيات المضبوطة في قسمي defaults و devices في ملف multipath.conf.

الجدول ٥-٤: خاصيات Multipath

الخاصية	الشرح
wwid	تحديد WWID لجهاز multipath الذي ستُطبَّق عليه خاصيات multipath، هذا الوسيط إلزاميٌ لهذا القسم من ملف multipath.conf.
alias	تحديد الاسم الرمزي لجهاز multipath الذي ستُطبَّق خاصيات multipath عليه، إذا كنت تستخدم user_friendly_names، فلا تضبط هذه القيمة إلى mpathn، هذا سيتداخل مع الاسم المُسنَد تلقائيًا وسيعطي أسماء عقد أجهزة غير صحيحة.

بالإضافة إلى ذلك، يمكن أن تتجاوز ضبط الخاصيات الآتية في قسم multipath:

- path_grouping_policy
- path_selector
- failback
- prio
- prio_args
- no_path_retry
- rr_min_io
- rr_weight
- flush_on_last_del

يُظهِر المثال الآتي خاصيات multipath المحددة في ملف الضبط لجهازي multipath محددَين، تكون قيمة WWID للجهاز الأول هي 3600508b4000156d70001200000b0000 واسمه الرمزي هو «yellow».

جهاز multipath الثاني في المثال له WWID بقيمة 1DEC_____321816758474 واسمه الرمزي هو «red»، وفي هذا المثال، ضبطت خاصية rr_weight إلى priorities.

```
multipaths {
        multipath {
                wwid
3600508b4000156d70001200000b0000
                alias                   yellow
                path_grouping_policy    multibus
                path_selector           "round-robin 0"
                failback                manual
                rr_weight               priorities
                no_path_retry           5
        }
        multipath {
                wwid
1DEC_____321816758474
                alias                   red
                rr_weight               priorities
          }
}
```

ه. ملف ضبط الأجهزة

جدول «خاصيات الأجهزة» الآتي يظهر الخاصيات التي يمكنك ضبطها لكل جهاز تخزين على حدة في قسم devices في ملف ضبط multipath.conf، تستخدم هذه الخاصيات من DM-Multipath ما لم تعاد كتابتها من الخاصيات المحددة في قسم multipaths في ملف multipath.conf للطرق التي تحتوي على الجهاز؛ هذه الخاصيات تتجاوز الخاصيات المضبوطة في قسم defaults في ملف multipath.conf.

العديد من الأجهزة التي تدعم تعدد الطرق مضمَّنة افتراضيًا في ملف ضبط multipath؛ القيم للأجهزة المدعومة افتراضيًا موجودةٌ في ملف multipath.conf.defaults.

ربما لا تحتاج إلى تعديل القيم لهذه الأجهزة، لكنك تستطيع تجاوز القيم الإضافية بتضمين قيد في ملف الضبط للجهاز، وإعادة كتابة هذه القيم، يمكنك نسخ قيم الضبط الافتراضية للجهاز من multipath.conf.annotated.gz أو إذا أردت الحصول على ملف ضبط مختصر، فراجع الملف multipath.conf.synthetic للجهاز وأعد كتابة القيم التي ترغب في تغييرها.

لإضافة جهاز إلى هذا القسم من ملف الإعدادات الذي لم يُضبَط افتراضيًا تلقائيًا، فعليك تحديد خاصيتَيّ vendor و product؛ تستطيع العثور على هذه القيم بالنظر في ملف /sys/block/device_name/device/vendor وفي /sys/block/device_name/model حيث device_name هو اسم الجهاز الذي سيستخدم في multipath، كما في المثال الآتي:

```
cat /sys/block/sda/device/vendor
WINSYS
cat /sys/block/sda/device/model
SF2372
```

الخاصيات الإضافية التي عليك تحديدها تعتمد على الجهاز الذي تعدّه، إذا كان الجهاز من نمط «فعال/فعال»، فلا تحتاج عادةً إلى أيّة خاصيات إضافية؛ لكن ربما تريد ضبط path_grouping_policy إلى القيمة multibus، فتكون الخاصيات التي قد تحتاج لها هي no_path_retry و rr_min_io، كما شُرِحَت في جدول «خاصيات Multipath».

أما إذا كان الجهاز من نمط «فعال/ غير فعال»، لكنه يُبدِّل تلقائيًا بين الطرق التي فيها دخل أو خرج إلى طريق غير فعال، فستحتاج إلى تعديل دالة التحقق إلى واحدة لا تُرسِل دخل أو خرج إلى الطرق لتختبر إذا كان يعمل (عدا ذلك، فسيستمر جهازك بالفشل)، هذا يعني أنه عليك ضبط قيمة path_checker دائمًا إلى القيمة tur؛ وهذا سيجدي نفعًا لجميع أجهزة SCSI التي تدعم Test Unit Ready (الذي تدعمه أغلبيتها).

إذا احتاج الجهاز إلى أمرٍ خاص لتبديل الطرق، فإن ضبط هذا الجهاز لاستخدام multipath يتطلب وحدة نواة لمتحكم العتاد، متحكم العتاد المتوفر حاليًا هو emc، وإذا لم يكن هذا كافيًا لجهازك، فربما لا تستطيع ضبط هذا الجهاز لاستخدام multipath.

الجدول ٥-٥: خاصيات الأجهزة

الخاصية	الشرح
vendor	تحديد اسم الشركة المصنعة لجهاز التخزين الذي تطبق عليه خاصيات الجهاز؛ على سبيل المثال COMPAQ.
product	تحديد اسم مُنتَج جهاز التخزين الذي تطبق عليه خاصيات الجهاز؛ على سبيل المثال HSV110 (C)COMPAQ.
revision	تحديد معرف revision لجهاز التخزين.
product_blacklist	تحديد التعبير النمطي المستخدم لحجب الأجهزة وفقًا للمُنتِج.
hardware_handler	تحديد الوحدة المستخدمة لتنفيذ أفعال خاصة بالعتاد عند تحويل مجموعات الطرق أو التعامل مع أخطاء الدخل أو الخرج؛ القيم الممكنة تتضمن: • القيمة 1 emc: المتحكم العتادي الخاص بمصفوفات EMC. • القيمة 1 alua: المتحكم العتادي الخاص بمصفوفات SCSI-3 ALUA. • القيمة 1 hp_sw: المتحكم العتادي الخاص بمتحكمات Compaq/HP. • القيمة 1 rdac: المتحكم العتادي الخاص بمتحكمات LSI/Engenio RDAC.

ويمكن إعادة كتابة الخاصيات الآتية في قسم device:

```
path_grouping_policy
getuid_callout
path_selector
path_checker
features
failback
prio
prio_args
no_path_retry
rr_min_io
rr_weight
fast_io_fail_tmo
dev_loss_tmo
flush_on_last_del
```

ملاحظة: عندما يحدد hardware_handler، فإن من مسؤوليتك التأكد من أن وحدة النواة الملائمة قد حُمِّلَت لدعم الواجهة (interface) المحددة، هذه الوحدة يمكن أن توجد في /lib/modules/`uname -r`/kernel/drivers/scsi/device_handler/، يجب أن تدمج الوحدة المطلوبة مع initd للتأكد من أن إمكانية الكشف والقدرة على تجاوز المشاكل موجودة أثناء وقت التشغيل، على سبيل المثال:

echo scsi_dh_alua >> /etc/initramfs-tools/modules ## append module to file
update-initramfs -u -k all

المثال الآتي يظهر قيد جهاز في ملف ضبط multipath:

```
#devices {
# device {
#   vendor      "COMPAQ    "
#   product      "MSA1000           "
#   path_grouping_policy multibus
#   path_checker tur
#   rr_weight  priorities
# }
#}
```

الفراغات المتروكة في حقول vendor، و product، و revision مهمة لأن multipath يجري مطابقة مباشرة لهذه الخاصيات، التي يكون تنسيقها معرفًا من مواصفات SCSI؛ وبشكل خاص الأمر «Standard INQUIRY»، فعندما تستخدم علامات الاقتباس، فإن حقول vendor، و product، و revision ستفسر بدقة كما هو محدد في المواصفات (spec)؛ يمكن تضمين التعابير النمطية في العبارات المقتبسة؛ وعندما يعرف حقلٌ ما بدون الفراغات المطلوبة، فسينسخ multipath السلسلة النصية إلى حافظة ذات سعة معينة وسيكمل الأحرف الباقية في الحافظة بعدد مناسب من الفراغات؛ حيث تتوقع المواصفات أن يكون الحقل كاملًا مملوءًا بعدد معين من المحارف أو الفراغات، كما في المثال السابق:

- حقل vendor: ٨ محارف.
- حقل product: ١٦ محرف.
- حقل revision: ٤ محارف.

لإنشاء ملف ضبط أكثر متانةً ومرونةً، فيمكن استخدام التعابير النمطية؛ تتضمن المعاملات القابلة للاستخدام:

«^$[].*?+»، تستطيع العثور على أمثلة عملية عن التعابير النمطية بمعاينة قاعدة بيانات multipath الحية، وملف ضبط multipath.conf، ملفات الأمثلة موجودة في /usr/share/doc/multipath-tools/examples:

```
# echo 'show config' | multipathd -k
```

٥. إدارة وإصلاح أخطاء DM-Multipath

ا. إعادة تحجيم جهاز Multipath أثناء عمله

إذا احتجت لإعادة تحجيم جهاز multipath أثناء عمله، فعليك اتباع الخطوات الآتية:

إعادة تحجيم الجهاز الفيزيائي، هذا الأمر متعلق بمنصة التخزين.

استخدام الأمر الآتي للعثور على طريق للوصول إلى LUN:

```
sudo multipath -l
```

إعادة تحجيم الطرق. في أجهزة SCSI، تؤدي كتابة ١ إلى ملف rescan إلى جعل الجهاز يطلب من محرك SCSI أن يعيد المسح، كما في الأمر الآتي:

```
# echo 1 > /sys/block/device_name/device/rescan
```

إعادة تحجيم جهاز multipath بتنفيذ أمر إعادة تحجيم multipathd:

```
sudo multipathd -k 'resize map mpatha'
```

إعادة تحجم نظام الملفات (باعتبار أننا لا نستخدم أيّة أقسام LVM أو DOS):

```
sudo resize2fs /dev/mapper/mpatha
```

ب. نقل جذر نظام الملفات من جهازٍ ذي طريقٍ واحدٍ إلى جهازٍ ذي طرقٍ متعددة

يمكن تبسيط هذه المهمة تبسيطًا شديدًا باستخدام UUID للتعرف على الأجهزة؛ بكل بساطة، ثبّت multipath-tools-boot وأعد الإقلاع؛ هذا سيعيد بناء قرص الذاكرة الابتدائي (initial ramdisk)، ويمنح multipath الفرصة لبناء الطرق قبل أن يوصل نظام الملفات الجذر باستخدام UUID.

ملاحظة: في كل مرة يحدث فيها multipath.conf يجب أن يُحدِّث initrd بتنفيذ الأمر update-initramfs -u -k all؛ السبب وراء نسخ multipath.conf إلى ramdisk هو إتمام عملية تحديد الأجهزة المتاحة للتجميع بواسطة القائمة السوداء وأقسام الأجهزة.

ج. نقل نظام ملفات ذاكرة التبديل من جهاز ذي طريقٍ واحدٍ إلى جهازٍ ذي طرقٍ متعددة

العملية تماثل تمامًا العملية المشروحة في القسم السابق «نقل جذر نظام الملفات من جهازٍ ذي طريقٍ واحدٍ إلى جهازٍ ذي طرقٍ متعددة».

د. العفريت Multipath

إذا وجدت مشكلة في تطبيق ضبط multipath، فعليك التأكد من أن عفريت multipath يعمل كما هو مشروح في «إعداد DM-Multipath»؛ يجب أن يعمل عفريت multipathd لكي تستطيع استخدام أجهزة multipathd. راجع أيضًا القسم «استكشاف الأخطاء وإصلاحها مع واجهة multipathd التفاعلية» الذي يشرح التفاعل مع multipathd للمساعدة في تنقيح الأخطاء.

ه. المشاكل مع queue_if_no_path

إذا ضُبِطَ "features "1 queue_if_no_path في ملف/etc/multipath.conf، فإن أي عملية تستخدم الدخل أو الخرج ستتوقف آنيًا إلى أن يُسترجَع طريقٌ أو أكثر؛ ولتجنب هذا، اضبط الخاصية no_path_retry N في ملف /etc/multipath.conf.

عند ضبط الخاصية no_path_retry، فاحذف الخيار "features "1 queue_if_no_path من ملف /etc/multipath.conf أيضًا، لكن إن كنت تستخدم جهازًا متعدد الطرق الذي تكون خاصية "features "1 queue_if_no_path متضمنة افتراضيًا في الضبط (وهذا حال الكثير من أجهزة SAN) فعليك إضافة "features "0 لتجاوز هذه الإعدادات الافتراضية، تستطيع فعل ذلك بنسخ قسم devices (فقط ذاك القسم، وليس كل الملف) من /usr/share/doc/multipath-tools/examples/multipath.conf.annotated.gz إلى /etc/multipath.conf وتعديله حسب احتياجاتك.

إذا احتجت لاستخدام الخيار "features "1 queue_if_no_path ولكنك عانيت من المشكلة المذكورة هنا، فاستخدم الأمر dmsetup لتعديل ضبط LUN معين أثناء التنفيذ؛ على سبيل المثال، إذا أردت تغيير الضبط في جهاز multipath المدعو mpathc من "queue_if_no_path" إلى "fail_if_no_path"، فنفذ الأمر الآتي:

```
sudo dmsetup message mpathc 0 "fail_if_no_path"
```

ملاحظة: عليك تحديد الاسم البديل mpathN بدلًا من المسار.

و. ناتج الأمر Multipath

إذا أنشأت أو عدلت أو عرضت جهاز multipath، فإنك ستحصل على مخرجات ضبط الجهاز الحالي؛ الصيغة هي الآتية (لكل جهاز multipath):

```
action_if_any: alias (wwid_if_different_from_alias)
↪ dm_device_name_if_known vendor,product
size=size features='features' hwhandler='hardware_handler'
↪ wp=write_permission_if_known
```

ولكل مجموعة طرق:

```
   -+- policy='scheduling_policy' prio=prio_if_known
   status=path_group_status_if_known
```

ولكل طريق:

```
     `- host:channel:id:lun devnode major:minor
dm_status_if_known path_status
   online_status
```

على سبيل المثال، مخرجات الأمر multipath ستظهر كالآتي:

```
   3600d0230000000000e13955cc3757800 dm-1 WINSYS,SF2372
   size=269G features='0' hwhandler='0' wp=rw
   |-+- policy='round-robin 0' prio=1 status=active
   | `- 6:0:0:0 sdb 8:16 active ready running
   `-+- policy='round-robin 0' prio=1 status=enabled
      `- 7:0:0:0 sdf 8:80        active ready     running
```

إذا كان الطريق مُعَدًّا وجاهزًا للدخل أو الخرج، فإن حالة الطريق هي ready أو ghost، وإن لم يكن يعمل الطريق، فإن الحالة هي faulty أو shaky؛ تُحدَّث حالة الطريق في كل فترة من الزمن بواسطة عفريت multipathd بالاعتماد على قيمة خاصية polling_interval المُعرَّفة في ملف /etc/multipath.conf.

حالة dm هي شبيهة بحالة الطريق، لكن من وجهة نظر النواة؛ حيث توجد قيمتين لحالة dm: failed، التي تكافئ faulty، و active التي تكافئ بقية الحالات. قد لا تتوافق في بعض الأحيان قيمة حالة الطريق وحالة dm.

قيم online_status الممكنة هي running و offline؛ حيث حالة offline تعني أن جهاز SCSI قد عُطِّل.

ملاحظة: عندما يُنشأ أو يُعدَّل جهاز multipath، فإن حالة مجموعة الطرق، واسم جهاز dm، وأذونات الكتابة، وحالة dm هي غير معلومة؛ وقد لا تكون الميزات (features) صحيحةً دومًا.

ز. طلبيات Multipath بالأمر multipath

يمكنك استخدام الخيارين l- و ll- للأمر multipath لعرض ضبط multipath الحالي، يعرض الخيار l- معلومات multipath المُجمَّعة من المعلومات الموجودة في sysfs وفي رابط الأجهزة، يعرض الخيار ll- المعلومات التي يعرضها l- بالإضافة إلى جميع مكونات النظام الأخرى.

عند عرض ضبط multipath، فإن هنالك ثلاثة مستويات من «الإسهاب»، التي يمكنك تحديدها بالخيار v- الخاص بالأمر multipath؛ بتحديد v0- فإن الأمر لا يعرض أيّة مخرجات، أما v1- فيعرض أسماء multipath المُنشأة أو المحدثة؛ التي يمكن أن تُمرَّر إلى أدوات أخرى

مثل kpartx؛ وبتحديد v2-، فإن الأمر يعرض جميع الطرق المكتشفة، و multipaths، وخرائط الأجهزة (device maps).

ملاحظة: يمكن تعديل درجة الإسهاب الافتراضية لأمر multipath (٢) بتعريف خاصية verbosity في قسم defaults في ملف multipath.conf.

يظهر المثال الآتي ناتج الأمر multipath -l:

```
sudo multipath -l
   3600d0230000000000e13955cc3757800 dm-1 WINSYS,SF2372
   size=269G features='0' hwhandler='0' wp=rw
   |-+- policy='round-robin 0' prio=1 status=active
   | `- 6:0:0:0 sdb 8:16        active ready     running
   `-+- policy='round-robin 0' prio=1 status=enabled
      `- 7:0:0:0 sdf 8:80        active ready     running
```

يعرض المثال الآتي ناتج الأمر multipath -ll:

```
sudo multipath -ll
   3600d0230000000000e13955cc3757801 dm-10 WINSYS,SF2372
   size=269G features='0' hwhandler='0' wp=rw
   |-+- policy='round-robin 0' prio=1 status=enabled
   | `- 19:0:0:1 sdc 8:32        active ready      running
   `-+- policy='round-robin 0' prio=1 status=enabled
     `- 18:0:0:1 sdh 8:112 active ready running
     3600d0230000000000e13955cc3757803 dm-2 WINSYS,SF2372
     size=125G features='0' hwhandler='0' wp=rw
     `-+- policy='round-robin 0' prio=1 status=active
       |- 19:0:0:3 sde 8:64 active ready running
          `- 18:0:0:3 sdj 8:144 active ready running
```

ح. خيارات الأمر Multipath

يشرح الجدول الآتي بعض خيارات الأمر multipath التي قد تجدها مفيدةً.

الجدول ٥-٦: خيارات مفيدة للأمر multipath

الخيار	الوصف
-l	عرض ضبط multipath الحالي المجمَّع من sysfs وروابط الأجهزة (device mapper).
-ll	عرض ضبط multipath الحالي المجمَّع من sysfs وروابط الأجهزة (device mapper)، وجميع مكونات النظام الأخرى.
-f device	إزالة جهاز multipath المسمى.
-F	إزالة جميع أجهزة multipath غير المستخدمة.

ط. تحديد قيود رابط الأجهزة بالأمر dmsetup

تستطيع استخدام الأمر dmsetup لمعرفة أيّة قيود لرابط الأجهزة تطابق أجهزة multipathd.

يعرض الأمر الآتي جميع أجهزة ربط الأجهزة، وكل أرقامهم الكبرى والصغرى؛ حيث تحدد الأرقام الصغرى اسم جهاز dm؛ على سبيل المثال، الرقم الصغير ٣ يطابق جهاز multipathd: /dev/dm-3:

```
sudo dmsetup ls
mpathd                 (253, 4)
mpathep1               (253, 12)
mpathfp1               (253, 11)
mpathb                 (253, 3)
mpathgp1               (253, 14)
mpathhp1               (253, 13)
mpatha                 (253, 2)
mpathh                 (253, 9)
mpathg                 (253, 8)
VolGroup00-LogVol01    (253, 1)
mpathf                 (253, 7)
VolGroup00-LogVol00    (253, 0)
mpathe                 (253, 6)
mpathbp1               (253, 10)
mpathd                 (253, 5)
```

ي. استكشاف الأخطاء وإصلاحها مع واجهة multipathd التفاعلية

إن الأمر multipathd -k هو واجهة تفاعلية للعفريت multipathd؛ ستظهر واجهة multipath التفاعلية بعد إدخال الأمر السابق، ويمكنك بعد تنفيذه أن تكتب help لعرض قائمة بالأوامر المتاحة، تستطيع إدخال أمر تفاعلي أو الضغط على Ctrl+D للخروج.

يمكن استخدام واجهة multipath التفاعلية لمعالجة الأخطاء التي قد تحصل مع نظامك؛ فعلى سبيل المثال، سلسلة الأوامر الآتية ستعرض ضبط multipath مع الإعدادات الافتراضية؛ راجع مقالة IBM ذات العنوان «Tricks with Multipathd» قبل إغلاقك للواجهة التفاعلية.

```
sudo multipathd -k
    > > show config
    > > CTRL-D
```

ستتأكد سلسلة الأوامر الآتية أن multipath قد حصل على آخر التعديلات في ملف multipath.conf:

```
sudo multipathd -k
> > reconfigure
> > CTRL-D
```

استخدام سلسلة الأوامر الآتية للتأكد من أن المتحقق من الطرق يعمل جيدًا:

```
sudo multipathd -k
> > show paths
> > CTRL-D
```

يمكن أيضًا تمرير الأوامر إلى multipathd باستخدام مجرى الدخل القياسي (stdin) كما يلي:

```
# echo 'show config' | multipathd -k
```

٦

الإدارة عن بعد

هنالك طرق عديدة لإدارة خادوم لينُكس عن بعد، سيشرح هذا الفصل ثلاثة من أشهر التطبيقات هي OpenSSH و Puppet و Zentyal.

١. خادوم OpenSSH

١. مقدمة

سنقدم في هذا القسم من دليل إدارة خواديم أوبنتو مجموعة أدوات فعّالة للتحكم البعيد ونقل الملفات بين الحواسيب المتصلة بالشبكة تسمى «OpenSSH»، سنتعلم أيضًا مجموعةً من إعدادات الضبط الممكنة مع خادوم OpenSSH ونتعلم كيف نغيرها في نظام أوبنتو الخاص بك.

إن OpenSSH هو إصدار مجاني وحر من مجموعة أدوات بروتوكول «الصدفة الآمنة» (Secure Shell [SSH]) للتحكم البعيد أو نقل الملفات بين الحواسيب؛ الأدوات التقليدية التي كانت مستخدمةً لإنجاز هذه المهام -مثل telnet أو rcp- لم تكن آمنةً حيث كانت تنقل كلمة مرور المستخدم بنصٍ واضح عند استخدامها؛ أما OpenSSH، فيُوفِّر عفريتًا وأدوات للعميل لإنشاء عمليات تحكم عن بعد أو نقل الملفات آمنة ومشفرة؛ ويستبدل الأدوات القديمة استبدالًا فعالًا.

مكونة خادوم OpenSSH المسماة sshd «تستمع» (listens) باستمرار لاتصالات العميل، وعندما يحدث طلب اتصال، فإن sshd يُنشِئ نوع الاتصال الصحيح اعتمادًا على نوع أداة العميل التي تجري الاتصال؛ على سبيل المثال، لو أن الحاسوب البعيد يتصل باستخدام برمجية عميل ssh، فإن خادوم OpenSSH يهيّء جلسة تحكم عن بُعد بَعد الاستيثاق؛ وإذا اتصل المستخدم البعيد مع خادوم OpenSSH باستخدام scp، فسيُهيّء عفريت خادوم OpenSSH نقلًا آمنًا للملفات بين الخادوم والعميل بعد الاستيثاق؛ ويمكن أن يَستخدِم OpenSSH عدّة طرق للاستيثاق، منها كلمة المرور العادية، والمفتاح العمومي (public key)، وبطاقات Kerberos للدخول.

ب. التثبيت

إن عمليـة تثـبيت خـادوم وعميـل OpenSSH هـي عمليـةٌ بسـيطة؛ اسـتخدم هـذا الأمـر من مِحَث الطرفية لتثبيت عميل OpenSSH على نظام أوبنتو:

```
sudo apt-get install openssh-client
```

استخدم هذا الأمر في سطر الأوامر لتثبيت خادوم OpenSSH، وملفات الدعم المتعلقة به:

```
sudo apt-get install openssh-server
```

يمكن أيضًا تحديد حزمة openssh-server للتثبيت أثناء عمليـة تثـبيت نسـخة الخـادوم من أوبنتو.

ج. الضبط

يمكنك ضبط السلوك الافتراضي لتطبيق خادوم OpenSSH (sshd) بتعديل الملف التالي /etc/ssh/sshd_config، للمزيد من المعلومات حول الضبط المستخدم في هذا الملف، تسـتطيع مراجعة صفحة الدليل الملائمة بإدخال الأمر الآتي في الطرفية:

```
man sshd_config
```

هنالك تعليمات كثيرة في ملف ضبط sshd تتحكم بأشياء مثل إعدادات الاتصالات وأنماط الاستيثاق؛ يمكن أن تُعدَّل ما سنشرحه من تعليمات الضبط بتعديل ملف /etc/ssh/sshd_config.

تنويه: قبل تعديل ملف الضبط، عليك أخذ نسخة من الملف الأصلي وحفظها من الكتابة عليها لكي تحصل على نسخة من الضبط الافتراضي كمرجع، ولإعادة استخدامها وقت الحاجة.

انسخ ملف /etc/ssh/sshd_config واحمهِ من الكتابة باستخدام الأوامر الآتية:

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.original
sudo chmod a-w /etc/ssh/sshd_config.original
```

ما يلي هو أمثلة عن تعليمات الضبط التي قد ترغب في تعديلها:

لضبط OpenSSH لكي يستمع على منفذ TCP ذو الرقم ٢٢٢٢ بدلًا من منفذ TCP الافتراضي ٢٢، فغيِّر تعليمة المنفذ كما يلي:

```
Port 2222
```

لتجعل sshd يسمح باستخدام الاستيثاق المبني على المفتاح العمومي، فأضف أو عدِّل السطر:

```
PubkeyAuthentication yes
```

إذا كان السطر موجودًا مسبقًا، فتأكد من عدم وجود رمز التعليق قبله.

لجعل خادوم OpenSSH يعرض محتويات ملف /etc/issue.net كلافتة قبل تسجيل الدخول، فأضف أو عدِّل السطر الآتي في ملف /etc/ssh/sshd_config:

```
Banner /etc/issue.net
```

بعد إجراء التعديلات على ملف /etc/ssh/sshd_config، فاحفظ الملف ثم أعد تشغيل خادوم sshd لتأخذ التغيرات مفعولها، وذلك بإدخال الأمر الآتي في مِحَث الطرفية:

```
sudo service ssh restart
```

تحذير: تتوفر المزيد من تعليمات الضبط لخادوم sshd لتعديل سلوك الخادوم لكي يلائم احتياجاتك، لكن يجب التنويه أنه إذا كانت الطريقة الوحيدة للوصول إلى الخادوم هي ssh، وارتكبت خطأً في ضبط sshd عبر ملف /etc/ssh/sshd_config، فستجد نفسك غير قادرٍ على الوصول إلى الخادوم بعد إعادة تشغيل خدمة sshd؛ بالإضافة إلى أنك إذا وضعت تعليمة ضبط خاطئة، فسيرفض خادوم sshd أن يعمل؛ لذلك كن حذرًا جدًا عند تعديل هذا الملف على خادوم بعيد.

د. مفاتيح SSH

تسمح مفاتيح SSH بالاستيثاق بين جهازين دون الحاجة إلى كلمة مرور، يَستخدم الاستيثاق بواسطة مفتاح SSH مفتاحين: مفتاح خاص (private) ومفتاح عام (public).

أدخِل الأمر الآتي في الطرفية لتوليد المفاتيح:

```
ssh-keygen -t dsa
```

سيولد الأمر السابق المفاتيح باستخدام خوارزمية التوقيع الرقمية (Digital Signature Algorithm [DSA])، ستُطلَب منك كلمة المرور أثناء العملية، بعد ذلك اضغط ببساطة على Enter لإنشاء المفتاح.

افتراضيًا، يُحفَظ المفتاح العام في الملف ~/.ssh/id_dsa.pub، بينما يكون ملف

‎~/.ssh/id_dsa هو المفتاح الخاص، انسخ ملف id_dsa.pub إلى المضيف البعيد، ثم أضفه إلى نهاية ملف ‎~/.ssh/authorized_keys باستخدام الأمر:

```
ssh-copy-id username@remotehost
```

في النهاية، تأكد من الأذونات على ملف authorized_keys، حيث يجب أن يملك المستخدم الموثوق فقط إذن القراءة والكتابة؛ إذا لم تكون الأذونات صحيحة، فعدلها بالأمر:

```
chmod 600 .ssh/authorized_keys
```

يجب أن تصبح الآن قادرًا على الدخول إلى SSH على المضيف البعيد دون طلب كلمة المرور.

٥. مصادر

- صفحة ويكي أوبنتو «SSH».
- موقع «OpenSSH».
- صفحة الويكي «Advanced OpenSSH».

٢. الأداة Puppet

Puppet هو إطار عمل متعدد المنصات يُمكّن مدراء النظام من إجراء المهام الشائعة باستخدام الكود؛ يمكن أن يقوم الكود بالعديد من المهام، من تثبيت برمجية جديدة إلى التحقق من أذونات الملفات، أو تحديث حسابات المستخدم؛ إن Puppet ليس رائعًا فقط أثناء عملية التثبيت الأساسية للنظام، بل أيضًا أثناء «دورة حياة النظام» بأكملها. يُستخدَم Puppet في معظم الحالات بنمط ضبط «خادوم/عميل».

سيغطي هذا القسم طريقة تثبيت وضبط Puppet كخادوم/عميل، سيشرح المثال البسيط الآتي طريقة تثبيت خادوم أباتشي باستخدام Puppet.

ا. التثبيت

أدخِل الأمر الآتي في طرفية الخادوم لتثبيت Puppet:

```
sudo apt-get install puppetmaster
```

وعلى جهاز أو أجهزة العميل؛ أدخِل الأمر:

```
sudo apt-get install puppet
```

ب. الضبط

قبل ضبط Puppet، ربما عليك إضافة سجل «DNS CNAME» من أجل النطاق puppet.example.com، حيث example.com هو النطاق الخاص بك؛ حيث يتحقق عملاء Puppet من سجل DNS للنطاق puppet.example.com كاسم خادوم Puppet، أو «Puppet Master»؛ راجع «الفصل الثامن: خدمة اسم النطاق (DNS)» لمزيدٍ من التفاصيل حول DNS.

إذا لم تشأ أن تستخدم DNS، فبإمكانك إضافة قيود إلى ملف /etc/hosts في الخادوم والعميل. على سبيل المثال، أضِف ما يلي في ملف /etc/hosts على خادوم Puppet:

```
127.0.0.1        localhost.localdomain localhost puppet
192.168.1.17     puppetclient.example.com puppetclient
```

وأضِف قيدًا للخادوم على كل عميل Puppet:

```
192.168.1.16     puppetmaster.example.com puppetmaster puppet
```

ملاحظة: استبدل عناوين IP الموجودة في المثال السابق بعناوين IP لخادومك وعملائك.

لنهيّء الآن بعض الموارد من أجل حزمة apache2، أنشئ الملف /etc/puppet/modules/apache2/manifests/init.pp الذي يحتوي الآتي:

```
package {
        'apache2':
               ensure => installed
}
service {
        'apache2':
               ensure => true,
               enable => true,
               require => Package['apache2']
}
```

أنشئ الآن الملف /etc/puppet/manifests/site.pp الذي يحتوي على:

```
node 'pupetclient.example.com' {
      include apache2
}
```

ملاحظة: استبدل pupetclient.example.com باسم مضيف عميل Puppet الحقيقي.

الخطوة النهائية لخادوم Puppet البسيط هي إعادة تشغيل العفريت:

```
sudo service puppetmaster restart
```

لقد أتممنا ضبط خادوم Puppet، حان الآن الوقت لضبط العميل.

أولًا، اضبط عفريت Puppetagent لكي يعمل، أي عدِّل ملف /etc/default/puppet مغيّرًا START إلى yes:

```
START=yes
```

ثم ابدأ تشغيل الخدمة:

```
sudo service puppet start
```

واعرض بصمة (fingerprint) شهادة العميل:

```
sudo puppet agent --fingerprint
```

وبالعودة إلى خادوم Puppet، اعرض طلبات توقيع الشهادات:

```
sudo puppet cert list
```

وفي خادوم Puppet، تأكد من بصمة العميل ووقِّع على شهادة العميل بكتابة:

```
sudo puppet sign pupetclient.example.com
```

وفي عميل Puppet، شغِّل برنامج puppet يدويًا في الأمامية (foreground)؛ هذه الخطوة ليست مطلوبة لكنها أفضل طريقة لاختبار وتنقيح عمل خدمة puppet.

```
sudo puppet agent --test
```

راجع /var/log/syslog لأيّة أخطاء بالضبط؛ إذا جرى كلُ شيءٍ على ما يرام، فستُثبَّت حزمة apache2 وجميع اعتمادياتها على عميل Puppet.

ملاحظة: هذا المثال بسيطٌ جدًا، ولا يُظهِر العديد من ميزات ومحاسن Puppet؛ راجع قسم المصادر للمزيد من المعلومات .

ج. مصادر

- توثيق موقع Puppet الرسمي.
- راجع أيضًا كتاب «Pro Puppet».
- مصدر آخر لمعلوماتٍ إضافية هو صفحة ويكي أوبنتو «Puppet».

٣. برمجية Zentyal

إن Zentyal هو خادوم لينُكس صغير موجَّه للأعمال (business server)، يمكن أن يُضبَط كبوابة، أو مدير بنى تحتية، أو «مدير تهديد موحد» (Unified Threat Manager)، أو خادوم مكتبي، أو خادوم اتصالات موحد، أو تجميعٌ مما سبق؛ جميع الخدمات الشبكية المُدارة من Zentyal تندمج مع بعضها اندماجًا كبيرًا، مؤتمِتًا معظم المهام، مما يساعد في تلافي الأخطاء في ضبط الشبكة والإدارة، ويسمح بتقليل الوقت اللازم لضبط البرمجيات؛ Zentyal هو برمجية مفتوحة المصدر، ومنشورة وفق رخصة غنو العمومية (GPL) وتعتمد على أوبنتو كأساسٍ لها.

تتضمن Zentyal سلسلةً من الحزم (حزمةٌ واحدةٌ عادةً لكل وحدة [module]) التي توفر واجهة ويب لضبط مختلف الخواديم أو الخدمات؛ ويُخزَّن الضبط في قاعدة بيانات Redis على نمط «مفتاح-قيمة»؛ لكن ضبط المستخدمين والمجموعات، والنطاقات (domains) يكون مبنيًا على OpenLDAP؛ وعندما تُضبَط أيّة خاصيات ضمن واجهة الويب، فستُعاد كتابة ملفات الإعدادات باستخدام قوالب ضبط مُوفَّرة من الوحدات؛ الميزة الأساسية من استخدام Zentyal هو واجهة رسومية موحدة لضبط جميع خدمات الشبكة مع دمجٍ ذي مستوىً عالٍ مع بعضها بعضًا.

ا. التثبيت

تتوفر إصدارة Zentyal 2.3 في مستودع Universe في أوبنتو ١٢.٠٤؛ الوحدات المتوفرة هي:

- zentyal-core و zentyal-common: أساس واجهة Zentyal والمكتبات الشائعة لإطار العمل؛ وتتضمن أيضًا السجلات (logs) ووحدات الأحداث (events modules) التي تعطي مدير النظام واجهة لمشاهدة السجلات، وتوليد أحداث منها.
- zentyal-network: إدارة إعدادات الشبكة، من البطاقات (داعمةً عناوين IP الثابتة، أو DHCP، أو VLAN، أوالجسور، أو PPPoE)، إلى البوابات المتعددة عندما يكون هنالك أكثر من اتصال بالإنترنت؛ وموازنة الحِمل والتوجيه المتقدم، وجداول التوجيه الثابتة، و DNS الديناميكي.
- zentyal-objects و zentyal-services: توفير طبقة تجريدية (abstraction level) لعناوين الشبكة (على سبيل المثال، LAN بدلًا من 192.168.1.0/24) والمنافذ مسماةً على أسماء خدماتها (مثلًا، HTTP بدلًا من TCP/٨٠).
- zentyal-firewall: ضبط قواعد iptables لحجب الاتصالات الممنوعة، واستخدام NAT وإعادة توجيه المنافذ.
- zentyal-ntp: تثبيت عفريت NTP لإبقاء ساعة الخادوم صحيحةً، وللسماح بعملاء الشبكة بمزامنة ساعاتهم مع ساعة الخادوم.
- zentyal-dhcp: ضبط خادوم ISC DHCP الذي يدعم مجالات الشبكة، وزمن «التأجير» الثابت، وغيرها من الخيارات المتقدمة مثل NTP، و WINS، و DNS الديناميكي، وإقلاع الشبكة مع PXE.

- zentyal-dns: إعداد خادوم ISC Bind9 على جهازك مع إمكانية التخزين المؤقت للطلبيات المحلية، أو كمُمرِّر، أو كخادوم استيثاق للنطاقات المضبوطة؛ ويسمح بضبط A، و CNAME، و MX، و NS، و TXT، وسجلات SRV.
- zentyal-ca: تضمين إدارة «سلطة الشهادات» (Certification Authority) مع Zentyal كي يتمكن المستخدمون من استخدام الشهادات للاستيثاق مع الخدمات، مثل OpenVPN.
- zentyal-openvpn: السماح بضبط عدة خواديم وعملاء VPN باستخدام OpenVPN مع ضبط ديناميكي للتوجيه باستخدام Quagga.
- zentyal-users: توفير واجهة لضبط وإدارة المستخدمين والمجموعات في OpenLDAP؛ الخدمات الأخرى في Zentyal تَستوثِق من المستخدمين باستخدام LDAP، مما يؤدي إلى وجود آلية مركزية لإدارة المستخدمين والمجموعات؛ من الممكن أيضًا مزامنة المستخدمين، وكلمات المرور، والمجموعات من خادوم Microsoft Active Directory.
- zentyal-squid: ضبط خدمتَيّ Squid و Dansguardian لتسريع التصفح، ويعود الفضل في ذلك إلى إمكانيات التخزين المؤقت وترشيح المحتوى.
- zentyal-samba: تسمح هذه الوحدة بضبط سامبا ودمجه مع ضبط LDAP موجود مسبقًا؛ ومن نفس الوحدة تستطيع تعريف سياسات لكلمات المرور، وإنشاء موارد مشتركة، وإسناد الأذونات.
- zentyal-printers: دمج CUPS مع سامبا والسماح، ليس فقط بضبط الطابعات، بل وإعطائها الأذونات بالاعتماد على مستخدمي ومجموعات LDAP.

لتثبيت Zentyal، افتح الطرفية في الخادوم واكتب (حيث <zentyal-module> هو اسم أحد الوحدات السابقة):

```
sudo apt-get install <zentyal-module>
```

ملاحظة: يُصدِر Zentyal إصدارًا واحدًا ثابتًا رئيسيًا في السنة (في أيلول/سبتمبر) مبنيٌ على آخر إصدارة أوبنتو طويلة الدعم (LTS)؛ يكون للإصدارات الثابتة أرقام رئيسية زوجية (مثلًا، ٢.٢ أو ٣.٠) والإصدارات التجريبية تكون أرقامها الرئيسية فردية (مثلًا ٢.١، و ٢.٣)؛ تأتي أوبنتو ١٢.٠٤ مع Zentyal بإصدار ٢.٣؛ إذا أردت الترقية إلى إصدارة ثابتة جديدة نُشِرَت بعد إصدار أوبنتو ١٢.٠٤، فيمكنك استخدم «Zentyal Team PPA»؛ قد توفر لك الترقية إلى الإصدارات الثابتة تصحيحات لعللٍ لم تصل إلى الإصدار ٢.٣ الموجود في أوبنتو ١٢.٠٤.

تنويه: إذا أردت المزيد من المعلومات حول إضافة الحزم من PPA؛ فراجع مقالة الويكي «Add a Personal Pachage Archive (PPA)».

ملحوظة جانبية، تستطيع إيجاد الحزم الآتية في Zentyal Team PPA، لكن ليس في مستودعات Universe في أوبنتو:

- وحدة zentyal-antivirus: تضمين مضاد الفيروسات ClamAV مع وحدات أخرى مثل الخادوم الوسيط (proxy) ومشاركة الملفات، أو mailfilter.
- وحدة zentyal-asterisk: ضبط Asterisk لتوفير PBX بسيط مبني على الاستيثاق بواسطة LDAP.
- وحدة zentyal-bwmonitor: السماح بمراقبة استهلاك التراسل الشبكي من قِبَل عملاء شبكتك المحلية.

- وحدة zentyal-captiveportal: تضمين «captive portal» مع الجدار الناري، ومستخدمي ومجموعات LDAP.
- وحدة zentyal-ebackup: السماح بإنشاء نسخ احتياطية مجدولة على خادومك باستخدام أداة النسخ الاحتياطي الشهيرة «duplicity».
- وحدة zentyal-ftp: ضبط خادوم FTP مع استيثاق مبني على LDAP.
- وحدة zentyal-ids: تضمين نظام اكتشاف التطفل في الشبكة.
- وحدة zentyal-ipsec: السماح بضبط أنفاق IPsec باستخدام OpenSwan.
- وحدة zentyal-jabber: تضمين خادوم XMPP مع مستخدمي ومجموعات LDAP.
- وحدة zentyal-thinclients: حل يعتمد على عملاء «رقيقين» (thin clients) مبني على LTSP.
- وحدة zentyal-mail: تشكيلة خدمات البريد الإلكتروني كاملة، بما فيها Postfix و Dovecot مع خلفية LDAP.
- وحدة zentyal-mailfilter: ضبط amavisd مع خدمات البريد الإلكتروني لترشيح الرسائل العشوائية (spam) والفيروسات المرفقة بالرسائل.
- وحدة zentyal-monitor: تضمين collectd لمراقبة أداء الخادوم والخدمات التي تعمل.
- وحدة zentyal-pptp: ضبط خادوم PPTP VPN.
- وحدة zentyal-raduis: تضمين FreeRADIUS مع مستخدمي ومجموعات LDAP.
- وحدة zentyal-software: واجهة بسيطة لإدارة وحدات Zentyal المثبتة، وتحديثات النظام.

- وحدة zentyal-trafficshaping: ضبط قواعد الحد من مرور البيانات للتضييق على التراسل الشبكي، وتحسين زمن التأخير (latency).
- وحدة zentyal-usercorner: السماح للمستخدمين بتعديل خاصيات LDAP الخاصة بهم باستخدام متصفح ويب.
- وحدة zentyal-virt: واجهة بسيطة لإنشاء وإدارة الأنظمة الوهمية المبنية على libvirt.
- وحدة zentyal-webmail: السماح بالوصول لبريدك عبر خدمة Roundcube webmail الشهيرة.
- وحدة zentyal-webserver: ضبط خادوم ويب أباتشي لاستضافة مختلف المواقع على جهازك.
- وحدة zentyal-zarafa: تضمين مجموعة Zarafa مع مجموعة Zentyal للبريد و LDAP.

ب. الخطوات الأولى

يُسمَح لأي حساب في النظام ينتمي للمجموعة sudo بتسجيل الدخول إلى واجهة Zentyal؛ إذا كنت تستخدم حساب المستخدم المُنشَأ أثناء التثبيت؛ فيجب أن يكون افتراضيًا في مجموعة sudo.

تنويه: إذا كنت تستخدم مستخدمًا آخرَ لا ينتمي للمجموعة sudo، فنفِّذ الأمر:

```
sudo adduser username sudo
```

للوصول إلى واجهة الويب (Zentyal)، فتوجه إلى /https://localhost (أو عنوان IP للخادوم البعيد)، ولأن Zentyal يستخدم شهادة SSL موقّعة ذاتيًا، فعليك إضافة استثناء له في متصفحك.

ستشاهد لوحة التحكم (dashboard) بعد تسجيل الدخول، مع لمحة عن خادومك؛ لضبط أيّة خاصية من خاصيات الوحدات المثبتة، فاذهب إلى الأقسام المختلفة في القائمة التي على اليسار؛ عندما تعدل أيّة تعديلات، فسيظهر زر أحمر مكتوب عليه «Save changes»، الذي عليك الضغط عليه لحفظ كل تعديلات الضبط؛ لتطبيق هذه التعديلات على خادومك، فيجب أن تفعّل الوحدة أولًا، وذلك من قيد «Module Status» على القائمة اليسرى؛ في كل مرة ستُفعِّل فيها وحدةً، فستظهر رسالة تطلب تأكيدك للقيام بالأفعال الضرورية، والتعديلات على خادومك وملفات ضبطه.

ملاحظة: إذا أردت تخصيص أي ملف ضبط لتنفيذ أفعال معينة (سكربتات أو أوامر) لضبط ميزات غير متوفرة في Zentyal، فضع قوالب ملفات الضبط المخصصة في /<etc/zentyal/stubs/<module/ و «hooks» في <etc/zentyal/hooks/<module>.<action/.

ج. مصادر

- صفحة توثيق Zentyal الرسمية.
- راجع أيضًا صفحة توثيق Zentyal الموفرة من المجتمع.
- لا تنسَ أيضًا زيارة المنتدى لدعم المجتمع، والتعقيبات، وطلبات الميزات ...إلخ.

٧

الاستيثاق الشبكي

يستخدم هذا الفصل LDAP للاستيثاق الشبكي Network authentication ومنح التصاريح.

١. خادوم OpenLDAP

البروتوكول الخفيف للوصول للدليل (Lightweight Directory Access Protocol) أو اختصارًا LDAP، هو بروتوكول لطلبيات وتعديل خدمة دليل مبني على X.500 يعمل عبر TCP/IP؛ الإصدارة الحالية من LDAP هي LDAPv3 كما هو معرَّف في RFC4510؛ والبرمجية المستخدمة في أوبنتو لتطبيق LDAPv3 هي OpenLDAP.

- هذه هي بعض المصطلحات والمفاهيم الأساسية:
- دليل LDAP هو شجرة من قيود البيانات (entries) التي تكون ذات هيكليّةٍ بطبيعتها، وتسمى شجرة معلومات الدليل (Directory Information Tree [DIT]).
- يتكون القيد من مجموعة من الخاصيات (attributes).
- الخاصية لها نوع (type) يكون اسمًا أو شرحًا؛ وقيمةٌ واحدةٌ أو أكثر.
- يجب أن تُعرِّف كل خاصية ما يسمى objectClass واحدًا على الأقل.
- الخاصيات و objectClasses مُعرَّفةٌ في مخططات (schemas) حيث يُعتبَر objectClass نوعًا خاصًا من الخاصيات.
- لكل قيد معرِّف خاص به هو «الاسم الفريد» (Distinguished Name [DN أو dn])؛ الذي يحتوي على «الاسم الفريد النسبي» (Relative Distinguished Name [RDN]) متبوعًا بالاسم الفريد للقيد الأب.
- الاسم الفريد للقيد ليس خاصيةً، بل يعتبر جزءًا من القيد نفسه.

ملاحظة: المصطلحات «الكائن» (object)، و«الحاوية» (container)، و«العقدة» (node) لها دلالات خاصة، لكنها أساسيًا تعني «قيد» (entry)؛ لكن «قيد» هو المصطلح الصحيح تقنيًا.

على سبيل المثال، لدينا هنا قيدٌ واحدٌ يحتوي على ١١ خاصية؛ ويكون اسمه الفريد «cn=John Doe,dc=example,dc=com»، واسمه الفريد النسبي (RDN) هو «cn=John Doe»، واسم الأب الفريد هو «dc=example,dc=com»:

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Larry Smith,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

القيد السابق مكتوب بصيغة LDIF (صيغة تبادل البيانات في LDAP [LDAP Data Interchange Format])؛ أيّة معلومات تضعها في شجرة معلومات الدليل (DIT) يجب أن تكون بهذه الصيغة؛ كما هي معرَّفة في RFC2849.

وعلى الرغم من أن هذا الفصل يستخدم LDAP للاستيثاق المركزي، لكنه يصلح لأي شيء فيه عدد كبير من طلبات الوصول لسندٍ خلفي (backend) تتمحور حول قراءة القيم المبنية على الخاصيات (name:value)؛ تتضمن الأمثلة على ذلك: دفترًا للعناوين، وقائمةً بعناوين البريد الإلكتروني، وضبطًا لخادوم البريد.

ا. التثبيت

لتثبيت عفريت خادوم OpenLDAP مع أدوات إدارة LDAP التقليدية؛ عليك تثبيت حزمتَيّ slapd و ldap-utils على التوالي وبالترتيب.

سيؤدي تثبيت slapd إلى إنشاء ضبط قادر على العمل مباشرةً؛ وخصوصًا إنشاء قاعدة بيانات تستطيع استخدامها لتخزين بياناتك؛ لكن اللاحقة (suffix أو DN الأساسية) ستُحدَّد من اسم نطاق الجهاز المحلي؛ إذا أردت شيئًا مختلفًا، فعدِّل ملف etc/hosts/ وبدِّل اسم النطاق باسمٍ ترغب في استخدامه كلاحقة؛ على سبيل المثال، إذا أردت أن تكون اللاحقة هي dc=example,dc=com، فعندها سيحتوي ملف hosts على سطرٍ شبيه بالآتي:

```
127.0.1.1         hostname.example.com hostname
```

تستطيع الرجوع إلى الإعدادات القديمة بعد تثبيت الحزمة.

ملاحظة: سيستخدم هذا الكتاب قاعدة بيانات ذات لاحقة dc=example,dc=com.

أكمل بتثبيت الحزمة:

```
sudo apt-get install slapd ldap-utils
```

منذ إصدارة أوبنتو ٨.١٠، صُمِّمَ slapd ليُضبَط داخل slapd نفسه، باستخدام DIT خاصة به لهذا الغرض مما يسمح بأن يُعدَّ slapd ديناميكيًّا دون الحاجة إلى إعادة تشغيل الخدمة؛ وستتكون قاعدة بيانات الضبط من مجموعة من ملفات LDIF النصية الموجودة في المجلد /etc/ldap/slapd.d؛ طريقة العمل هذه معروفةٌ بعدَّة أسماء: طريقة slapd-config، وطريقة RTC ‏(Real Time Configuration)، أو طريقة cn=config؛ ما زلتَ تستطيع استخدام ملف الضبط التقليدي slapd.conf لكن هذه الطريقة غير مستحسنة؛ وستلغى هذه الميزة تدريجيًا.

ملاحظة: تستخدم أوبنتو طريقة slapd-config لضبط slapd، وكذلك سيستخدمها هذا الكتاب.

سيُطلَب منك أثناء التثبيت تعريف «الأوراق الاعتمادية الإدارية» ‏(administrative credentials)؛ وهي الأوراق الاعتمادية المبنية على LDAP لقاعدة rootDN؛ افتراضيًا، يكون DN للمستخدم هو cn=admin,dc=example, dc=com؛ وأيضًا افتراضيًا لا يُنشَأ حساب إداري لقاعدة بيانات slapd-config؛ لذا عليك الاستيثاق خارجيًا للوصول إلى LDAP وسنرى كيفية فعل ذلك لاحقًا.

تأتي بعض المخططات الكلاسيكية (cosine و nis و inetorgperson) افتراضيًا مع slapd هذه الأيام؛ وهنالك أيضًا مخطط «core» المطلوب ليعمل أي مخطط آخر.

ب. ما يجب فعله بعد التثبيت

تُعِدّ عملية التثبيت شجرتين لمعلومات الدليل؛ واحدة لاستخدامها في ضبط slapd (slapd-config) وواحدة لبياناتك الشخصية (dc=example,dc=com)؛ لنلقِ نظرةً.

هذا ما تبدو عليه قاعدة بيانات slapd-config؛ تذكَّر أن هذه القاعدة مبنية على LDIF وموجودة في /etc/ldap/slapd.d:

```
/etc/ldap/slapd.d/
/etc/ldap/slapd.d/cn=config
/etc/ldap/slapd.d/cn=config/cn=module{0}.ldif
/etc/ldap/slapd.d/cn=config/cn=schema
/etc/ldap/slapd.d/cn=config/cn=schema/cn={0}core.ldif
/etc/ldap/slapd.d/cn=config/cn=schema/cn={1}cosine.ldif
/etc/ldap/slapd.d/cn=config/cn=schema/cn={2}nis.ldif
/etc/ldap/slapd.d/cn=config/cn=schema/cn={3}inetorgperson.ldif
/etc/ldap/slapd.d/cn=config/cn=schema.ldif
/etc/ldap/slapd.d/cn=config/olcBackend={0}hdb.ldif
/etc/ldap/slapd.d/cn=config/olcDatabase={0}config.ldif
/etc/ldap/slapd.d/cn=config/olcDatabase={-1}frontend.ldif
/etc/ldap/slapd.d/cn=config/olcDatabase={1}hdb.ldif
/etc/ldap/slapd.d/cn=config.ldif
```

ملاحظة: لا تُعدِّل قاعدة بيانات slapd-config مباشرةً، أجرِ التعديلات باستخدام بروتوكول LDAP (عبر الأدوات الخاصة).

تنويه: في نسخة خادوم أوبنتو ١٤.١٠ وربما ما بعدها، قد لا يعمل الأمر الآتي بسبب علّة.

وهذا ما تبدو عليه شجرة معلومات الدليل slapd-config عند طلبها بواسطة بروتوكول LDAP:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config dn

dn: cn=config
dn: cn=module{0},cn=config
dn: cn=schema,cn=config
dn: cn={0}core,cn=schema,cn=config
dn: cn={1}cosine,cn=schema,cn=config
dn: cn={2}nis,cn=schema,cn=config
dn: cn={3}inetorgperson,cn=schema,cn=config
dn: olcBackend={0}hdb,cn=config
dn: olcDatabase={-1}frontend,cn=config
dn: olcDatabase={0}config,cn=config
dn: olcDatabase={1}hdb,cn=config
```

شرح القيود السابقة:

- cn=config: الإعدادات العامة.
- cn=module{0},cn=config: وحدة مُحَمَّلة ديناميكيًا.
- cn=schema,cn=config: يحتوي على مخطط مستوى النظام (hard-coded).
- cn={0}core,cn=schema,cn=config: يحتوي على مخطط الأساس (hard-coded).
- cn={1}cosine,cn=schema,cn=config: المخطط cosine.
- cn={3}inetorgperson,cn=schema,cn=config: المخطط inetorgperson.
- olcBackend={0}hdb,cn=config: نوع تخزين 'hdb'.
- olcDatabase={-1}frontend,cn=config: قاعدة بيانات الواجهة (frontend)، الضبط الافتراضي لقواعد البيانات الأخرى.
- olcDatabase={0}config,cn=config: قاعدة بيانات ضبط slapd (cn=config).
- olcDatabase={1}hdb,cn=config: نسخة قاعدة البيانات الخاصة بك (dc=example,dc=com).

وهذا ما تبدو عليه شجرة معلومات الدليل dc=example,dc=com:

```
ldapsearch -x -LLL -H ldap:/// -b dc=example,dc=com dn
dn: dc=example,dc=com
dn: cn=admin,dc=example,dc=com
```

شرح القيود السابقة:

- dc=example,dc=com: أساس DIT.
- cn=admin,dc=example,dc=com: المدير (rootDN) لشجرة معلومات الدليل هذه (ضُبِط أثناء تثبيت الحزمة).

ج. تعديل وملء قاعدة البيانات

لنضع بعض المحتويات في قاعدة البيانات؛ حيث سنضيف الآتي:

- عقدة اسمها People (لتخزين المستخدمين).
- عقدة اسمها Groups (لتخزين المجموعات).
- مجموعة اسمها miners.
- مستخدم اسمه john.

أنشئ ملف LDIF وسَمِّه add_content.ldif:

```
dn: ou=People,dc=example,dc=com
objectClass: organizationalUnit
ou: People

dn: ou=Groups,dc=example,dc=com
objectClass: organizationalUnit
ou: Groups

dn: cn=miners,ou=Groups,dc=example,dc=com
objectClass: posixGroup
cn: miners

gidNumber: 5000
dn: uid=john,ou=People,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: john
sn: Doe
givenName: John
cn: John Doe
displayName: John Doe
uidNumber: 10000
gidNumber: 5000
userPassword: johnldap
gecos: John Doe
loginShell: /bin/bash
homeDirectory: /home/john
```

ملاحظة: من المهم ألّا تتصادم قيم uid و gid في دليلك مع القيم المحلية؛ استخدم مجالات الأرقام الكبيرة؛ فابدأ مثلًا من ٥٠٠٠، وبتكبير قيم uid و gid في ldap، فإنك تسمح أيضًا بسهولة التحكم في ماذا يستطيع أن يفعله المستخدم المحلي، في مقابل ما يفعله مستخدم ldap؛ سنفصِّل هذا الموضوع لاحقًا.

أضف المحتويات:

```
ldapadd -x -D cn=admin,dc=example,dc=com -W -f add_content.ldif

Enter LDAP Password: ********
adding new entry "ou=People,dc=example,dc=com"

adding new entry "ou=Groups,dc=example,dc=com"

adding new entry "cn=miners,ou=Groups,dc=example,dc=com"

adding new entry "uid=john,ou=People,dc=example,dc=com"
```

سنتحقق من إضافة المعلومات إضافةً صحيحةً باستخدام الأداة ldapsearch:

```
ldapsearch -x -LLL -b dc=example,dc=com 'uid=john' cn gidNumber

dn: uid=john,ou=People,dc=example,dc=com
cn: John Doe
gidNumber: 5000
```

شرح ماذا حصل:

- x-: ربط بسيط؛ لن تُستخدَم طريقة SASL الافتراضية.
- LLL-: تعطيل طباعة معلوماتٍ إضافيةً.
- uid=john: «مُرَشِّح» (filter) للعثور على المستخدم john.
- cn gidNumber: طلب خاصيات معينة لإظهارها (القيمة الافتراضية هي إظهار جميع الخاصيات).

د. تعديل قاعدة بيانات slapd

يمكن أن تُطلَب أو تُعدَّل شجرة دليل المعلومات الخاصة بضبط slapd ‏(slapd-config)؛ سنذكر هنا بعض الأمثلة:

استخدم الأمر idapmodify لإضافة «فهرس» (خاصية DbIndex) إلى قاعدة بيانات {1}hdb,cn=config (التي هي dc=example,dc=com)؛ أنشِئ ملفًا اسمه uid_index.ldif فيه المحتويات الآتية:

```
dn: olcDatabase={1}hdb,cn=config
add: olcDbIndex
olcDbIndex: uid eq,pres,sub
```

ثم نفِّذ الأمر:

```
sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f uid_index.ldif

modifying entry "olcDatabase={1}hdb,cn=config"
```

تستطيع تأكيد التغيير بهذه الطريقة:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
cn=config '(olcDatabase={1}hdb)' olcDbIndex

dn: olcDatabase={1}hdb,cn=config
olcDbIndex: objectClass eq
olcDbIndex: uid eq,pres,sub
```

لنضف الآن مخططًا (schema)، يجب أولًا أن تحوَّل إلى صيغة LDIF؛ تستطيع إيجاد مخططات مُحوَّلة، وغير مُحوَّلة في مجلد /etc/ldap/schema.

ملاحظة: حذف المخططات من قاعدة بيانات slapd-config ليس أمرًا بسيطًا؛ تدرب على إضافة المخططات على نظام خاص بالتجارب.

قبل إضافة أيّة مخططات، يجب أن تتحقق من أيّة مخططات قد ثُبِّتَت مسبقًا (المخرجات الآتية هي المخرجات الافتراضية [out-of-the-box]):

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
cn=schema,cn=config dn

dn: cn=schema,cn=config
dn: cn={0}core,cn=schema,cn=config
dn: cn={1}cosine,cn=schema,cn=config
dn: cn={2}nis,cn=schema,cn=config
dn: cn={3}inetorgperson,cn=schema,cn=config
```

سنضيف مخطط CORBA في المثال الآتي:

أنشِئ ملف ضبط التحويل المسمى schema_convert.conf يتضمن الأسطر الآتية:

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/collective.schema
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/duaconf.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema
include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/ldapns.schema
include /etc/ldap/schema/pmi.schema
```

أنشِئ مجلد المخرجات ldif_output.

حدد فهرس المخطط:

```
slapcat -f schema_convert.conf -F ldif_output \
-n 0 | grep corba,cn=schema

cn={1}corba,cn=schema,cn=config
```

ملاحظة: عندما «يحقن» (injects) slapd الكائنات التي لها نفس الاسم الفريد للأب؛ فإنه سيُنشِئ فهرسًا لهذا الكائن؛ ويحتوى الفهرس ضمن قوسين معقوفين: {X}.

استخدم slapcat للقيام بالتحويل:

```
slapcat -f schema_convert.conf -F ldif_output -n0 -H \
ldap:///cn={1}corba,cn=schema,cn=config -l cn=corba.ldif
```

المخطط المحوّل موجودٌ الآن في cn=corba.ldif.

عدِّل cn=corba.ldif حتى تصل إلى الخاصيات الآتية:

```
dn: cn=corba,cn=schema,cn=config
...
cn: corba
```

أزل الآن الأسطر الآتية من النهاية:

```
structuralObjectClass: olcSchemaConfig
entryUUID: 52109a02-66ab-1030-8be2-bbf166230478
creatorsName: cn=config
createTimestamp: 20110829165435Z
entryCSN: 20110829165435.935248Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20110829165435Z
```

قد تختلف قيم الإعدادات عندك.

في النهاية، استخدم ldapadd لإضافة مخطط جديد إلى شجرة معلومات دليل slapd-config:

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f cn=corba.ldif

adding new entry "cn=corba,cn=schema,cn=config"
```

تأكد من المخططات المُحَمَّلة:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL \
-H ldapi:/// -b cn=schema,cn=config dn

dn: cn=schema,cn=config
dn: cn={0}core,cn=schema,cn=config
dn: cn={1}cosine,cn=schema,cn=config
dn: cn={2}nis,cn=schema,cn=config
dn: cn={3}inetorgperson,cn=schema,cn=config
dn: cn={4}corba,cn=schema,cn=config
```

ملاحظة: لكي يستوثق العملاء والتطبيقات الخارجية باستخدام LDAP، فإن عليك ضبط كل واحد منهم ليفعل ذلك؛ راجع توثيق تلك العملاء لمعلومات ملائمة عنهم.

ه. التسجيل (Logging)

لا غنى عن تفعيل تسجيل slapd عند استخدام تطبيقات تعتمد على OpenLDAP، لكن عليك تفعيله يدويًا بعد تثبيت البرمجيات؛ وإذا لم تفعل ذلك، فستظهر رسائل بدائية غير مفيدة فقط في السجلات؛ ويُفعَّل التسجيل، كغيره من ضبط slapd، عبر قاعدة بيانات slapd-config.

يأتي OpenLDAP مع عدّة أنظمة فرعية للتسجيل (مستويات)، تحتوي كلٌ منها على المستوى الأدنى منها؛ مستوى جيد للتجربة هو stats؛ هنالك المزيد من المعلومات حول الأنظمة الفرعية المختلفة في صفحة دليل man slapd-config.

أنشِئ ملف logging.ldif بالمحتويات الآتية:

```
dn: cn=config
changetype: modify
add: olcLogLevel
olcLogLevel: stats
```

طبِّق التعديل:

```
sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f logging.ldif
```

وهذا ما سيُنتِج كميّةً كبيرةً من السجلات؛ وربما تحتاج للعودة وتقليل درجة الإسهاب عندما يصبح نظامك نظامًا إنتاجيًا (in production)، لكن ربما يجعل ضبط الإسهاب هذا محرك syslog في نظامك يعاني من كثرة الرسائل، وقد يتجاوز بعضها دون تسجيله:

```
rsyslogd-2177: imuxsock lost 228 messages from pid 2547 due to
rate-limiting
```

قد تفكر في تغيير ضبط rsyslog؛ ضع في ملف /etc/rsyslog.conf:

```
# Disable rate limiting
# (default is 200 messages in 5 seconds; below we make the 5
become 0)
$SystemLogRateLimitInterval 0
```

ثم أعد تشغيل عفريت rsyslog:

```
sudo service rsyslog restart
```

و. التناسخ

تتزايد أهمية خدمة LDAP عندما تزداد أنظمة الشبكات المُعتَمِدة عليها؛ تكون الممارسات العملية القياسية -في مثل هذه البيئة- هي بناء redundancy في LDAP لمنع توقف الخدمات إذا لم يعد يستجيب خادوم LDAP؛ يتم ذلك باستخدام تناسخ LDAP؛ نصل إلى التناسخ باستخدام محرك Syncrepl؛ الذي يسمح بمزامنة التغيرات باستخدام موديل «مستهلك-مزود»؛ نوع التناسخ الذي سنستخدمه في هذا الكتاب هو دمج للنوعين الآتيين: refreshAndPersist، و delta-syncrepl؛ الذي يُرسِل فيه المزود القيود إلى المستهلك عند إنشائهم مباشرةً؛ بالإضافة إلى أنه لا تُرسَل جميع القيود، وإنما التغيرات التي حصلت فقط.

ضبط المزود

سنبدأ بضبط المزود (Provider):

أنشِئ ملف LDIF بالمحتويات الآتية وسمِّه provider_sync.ldif:

```
# Add indexes to the frontend db.
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryCSN eq
-
add: olcDbIndex
olcDbIndex: entryUUID eq

#Load the syncprov and accesslog modules.
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov
-
```

```
add: olcModuleLoad
olcModuleLoad: accesslog

# Accesslog database definitions
dn: olcDatabase={2}hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {2}hdb
olcDbDirectory: /var/lib/ldap/accesslog
olcSuffix: cn=accesslog
olcRootDN: cn=admin,dc=example,dc=com
olcDbIndex: default eq
olcDbIndex: entryCSN,objectClass,reqEnd,reqResult,reqStart

# Accesslog db syncprov.
dn: olcOverlay=syncprov,olcDatabase={2}hdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE
olcSpReloadHint: TRUE

# syncrepl Provider for primary db
dn: olcOverlay=syncprov,olcDatabase={1}hdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE

# accesslog overlay definitions for primary db
dn: olcOverlay=accesslog,olcDatabase={1}hdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcAccessLogConfig
olcOverlay: accesslog
olcAccessLogDB: cn=accesslog
olcAccessLogOps: writes
olcAccessLogSuccess: TRUE

# scan the accesslog DB every day, and purge entries older than
7 days
olcAccessLogPurge: 07+00:00 01+00:00
```

غيّر قيمة rootDN في ملف LDIF ليُطابِق الذي عندك في الدليل.

لا يجب تعديل إعدادات apparmor لبرمجية slapd لتحديد موقع قاعدة بيانات accesslog، لأن الملف /etc/apparmor/local/usr.sbin.slapd يحتوي على الأسطر الآتية:

```
/var/lib/ldap/accesslog/ r,
/var/lib/ldap/accesslog/** rwk,
```

أنشِئ مجلدًا، وهيّء ملف ضبط قاعدة البيانات، وأعد تحميل apparmor:

```
sudo -u openldap mkdir /var/lib/ldap/accesslog
sudo -u openldap cp /var/lib/ldap/DB_CONFIG \
/var/lib/ldap/accesslog
sudo service apparmor reload
```

أضف المحتويات الجديدة؛ وأعد تشغيل العفريت بسبب التعديل في apparmor:

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f provider_sync.ldif
sudo service slapd restart
```

لقد ضُبِطَ المزود بنجاح.

ضبط المستهلك

عليك الآن ضبط المستهلك.

تثبيت البرمجية باتباع تعليمات قسم «التثبيت»؛ وتأكد أن قاعدة بيانات slapd-config مماثلة للمزود؛ وتحديدًا تأكد من أن المخططات ولاحقة قاعدة البيانات هي نفسها.

أنشِئ ملف LDIF بالمحتويات الآتية وسمّه consumer_sync.ldif:

```
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov

dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryUUID eq
-
add: olcSyncRepl
olcSyncRepl: rid=0 provider=ldap://ldap01.example.com
bindmethod=simple binddn="cn=admin,dc=exa
credentials=secret searchbase="dc=example,dc=com"
logbase="cn=accesslog"
logfilter="(&(objectClass=auditWriteObject)(reqResult=0))"
schemachecking=on
type=refreshAndPersist retry="60 +" syncdata=accesslog
-
add: olcUpdateRef
olcUpdateRef: ldap://ldap01.example.com
```

تأكد أن قيم الخاصيات الآتية صحيحة:

- provider (اسم مضيف المزود -ldap01.example.com في هذا المثال- أو عنوان IP).
- binddn (الاسم الفريد للمدير الذي تستخدمه).
- credentials (كلمة مرور المدير الذي تستخدمه).
- searchbase (لاحقة قاعدة البيانات التي تستخدمها).
- olcUpdateRef (اسم مضيف أو عنوان IP لخادوم المزود).
- rid («Replica Id» عدد من ثلاثة أرقام يعرف النسخة، يجب أن يكون لكل مستهلك رقم rid واحد على الأقل).

أضف المحتويات الجديدة:

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f consumer_sync.ldif
```

لقد انتهيت، يجب أن يبدأ الآن تزامن قاعدتَيّ البيانات (ذاتَيّ اللاحقة dc=example,dc=com).

الاختبار

بعد بدء الاستنساخ، تستطيع مراقبته بتشغيل الأمر:

```
ldapsearch -z1 -LLLQY EXTERNAL -H ldapi:/// -s base contextCSN

dn: dc=example,dc=com
contextCSN: 20120201193408.178454Z#000000#000#000000
```

عندما تتوافق المخرجات في المزود والمستهلك (#20120201193408.178454Z 000000#000#000000 في المثال السابق) في كلا الجهازين؛ فستكون عملية الاستنساخ قد تمَّت؛ وفي كل مرة يُجرى فيها تعديل في المزود، فإن القيمة ستُعدَّل وكذلك يجب أن تُعدَّل قيمة ناتج الأمر السابق في المستهلك أو المستهلكين.

إذا كان اتصالك ضعيفًا، أو كان حجم قاعدة بيانات ldap كبيرًا، فربما يحتاج contextCSN في المستهلك وقتًا ليطابق مثيله في المزود؛ لكنك تعلم أن العملية قيد الإجراء لأن contextCSN في المستهلك يزداد مع الزمن.

إذا كان contextCSN في المستهلك مفقودًا، أو كان لا يطابق المزود؛ فعليك إيقاف العملية والبحث عن سبب المشكلة قبل الإكمال، جرب التحقق من سجلات slapd (syslog) وملفات auth في المزود للتأكد فيما إذا كانت طلبات الاستيثاق من المستهلك قد نجحت أم لا؛ وفيما إذا أعادت طلبياته للحصول على بيانات (ستشبه عبارات ldapsearch كثيرًا) أيّة أخطاء.

لاختبار إذا كان يعمل؛ جرب طلب DN في قاعدة البيانات في المستهلك:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL \
-H ldapi:/// -b dc=example,dc=com dn
```

يجب أن تشاهد المستخدم «john» والمجموعة «miners» بالإضافة إلى عقدتَيّ «People» و «Groups».

ز. التحكم في الوصول

إدارة أي نوع من الوصول (قراءة، أو كتابة ...إلخ.) التي يجب أن يحصل عليها المستخدمون للموارد تدعى «التحكم في الوصول» (access control)؛ تعليمات الضبط المستخدمة تسمى «قوائم التحكم في الوصول» (access control lists) أو ACL.

عندما تُثبّت حزمة slapd، فستُضبَط قوائم مختلفة للتحكم في الوصول؛ سنلقي نظرةً على بعض نتائج هذه القيم الافتراضية؛ وسنحصل بذلك على فكرة عن كيفية عمل قوائم التحكم بالوصول وكيفية ضبطها.

لكي نحصل على ACL فعال لطلبية LDAP، فسنحتاج إلى أن ننظر إلى سجلات قوائم التحكم بالوصول لقاعدة البيانات التي تُجرى الطلبيات عليها، بالإضافة إلى واجهة أمامية (frontend) خاصة لقاعدة البيانات؛ قوائم التحكم بالوصول المتعلقة بالنقطة الأخيرة تسلك سلوكًا افتراضيًا في حالة لم تتطابق النقطة الأولى؛ الواجهة الأمامية لقاعدة البيانات هي ثاني ما «تنظر» إليه قوائم التحكم بالوصول؛ وأول ما ستُطبِّقه قوائم التحكم بالوصول هو أول ما سُيطابَق («first match wins») بين مصدرَيّ قوائم التحكم بالوصول السابقَين؛ ستعطي الأوامر الآتية، على التوالي وبالترتيب، قيم ACL لقاعدة بيانات hdb («dc=example,dc=com») والقيم المتعلقة بالواجهة الأمامية لقاعدة البيانات:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
cn=config '(olcDatabase={1}hdb)' olcAccess

dn: olcDatabase={1}hdb,cn=config
olcAccess: {0}to attrs=userPassword,shadowLastChange by self
write by anonymous
auth by dn="cn=admin,dc=example,dc=com" write by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by self write by
dn="cn=admin,dc=example,dc=com" write by * read
```

ملاحظة: يملك rootDN دائمًا جميع الحقوق لقاعدة بياناته؛ تضمينها في قوائم التحكم بالوصول يوفر توضيحًا للضبط؛ لكنه يؤدي إلى تخفيض في أداء slapd.

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
cn=config '(olcDatabase={-1}frontend)' olcAccess

dn: olcDatabase={-1}frontend,cn=config
olcAccess: {0}to * by
dn.exact=gidNumber=0+uidNumber=0,cn=peercred,
cn=external,cn=auth manage by * break
olcAccess: {1}to dn.exact="" by * read
olcAccess: {2}to dn.base="cn=Subschema" by * read
```

أول قائمة تحكم بالوصول هي مهمة ومحورية:

```
olcAccess: {0}to attrs=userPassword,shadowLastChange by self
write by anonymous auth by dn="cn=admin,dc=example,dc=com"
write by * none
```

يمكن أن يعبر عنها بطريقة أخرى لتسهيل فهمها:

```
to attrs=userPassword
 by self write
 by anonymous auth
 by dn="cn=admin,dc=example,dc=com" write
 by * none

to attrs=shadowLastChange
 by self write
 by anonymous auth
 by dn="cn=admin,dc=example,dc=com" write
 by * none
```

تركيبة قوائم التحكم بالوصول (هنالك قاعدتين) تجبر ما يلي:

الوصول المجهول 'auth' موفر إلى خاصية userPassword لكي يتم الاتصال الابتدائي؛ ربما هذا عكس البديهي، نحتاج إلى 'by anonymous auth' حتى لو لم نكن نريد الوصول المجهول إلى شجرة بيانات الدليل. بعد أن تتصل النهاية البعيدة، فعندها يمكن أن يقع الاستيثاق (انظر النقطة الآتية).

يمكن أن يحدث الاستيثاق لأن جميع المستخدمين لديهم وصول 'read' (بسبب 'by self write') لخاصية userPassword.

عدا ذلك، فلا يمكن الوصول إلى خاصية userPassword من أي مستخدمين آخرين؛ مع استثناء rootDN، الذي يملك وصولًا كاملًا إليها.

لكي يغير المستخدمون كلمات مرورهم، باستخدام passwd أو غيرها من الأدوات، فإن خاصية shadowLastChange يجب أن تكون متاحةً بعد الاستيثاق من المستخدم.

يمكن البحث في شجرة DIT السابقة بسبب 'by * read' في:

```
to *
 by self write
 by dn="cn=admin,dc=example,dc=com" write
 by * read
```

إذا لم يكن هذا مرغوبًا فعليك تعديل ACL؛ ولكي يكون الاستيثاق جبريًا أثناء طلب bind، فيمكنك بشكل بديل (أو بالمشاركة مع ACL المعدلة) استخدام التعليمة 'olcRequire: authc'.

وكما ذُكِر سابقًا، لا يوجد حساب إدارة مُنشَأ لقاعدة بيانات slapd-config. لكن هنالك هوية SASL التي تملك الوصول الكامل إليها؛ والتي تمثل root أو sudo؛ ها هي ذا:

```
dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
```

سيعرض الأمر الآتي قوائم التحكم بالوصول (ACLs) لقاعدة بيانات slapd-config:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
cn=config '(olcDatabase={0}config)' olcAccess

dn: olcDatabase={0}config,cn=config
olcAccess: {0}to * by
dn.exact=gidNumber=0+uidNumber=0,cn=peercred,
cn=external,cn=auth manage by * break
```

ولما كانت هذه هوية SASL، فإننا نحتاج إلى استخدام آلية SASL عندما نستخدم أداة LDAP كما رأينا ذلك للعديد من المرات في هذا الكتاب؛ هذه الآلية خارجية؛ انظر إلى الأمر السابق كمثال، لاحظ أنه:

١. يجب أن تستخدم sudo لكي تصبح بهوية الجذر لكي تطابق قوائم التحكم بالوصول.

٢. الآلية الخارجية (EXTERNAL) تعمل باستخدام IPC (مقابل نطاقات UNIX) الذي يعني أنه عليك استخدام صيغة ldapi URI.

طريقة موجزة للحصول على جميع قوائم التحكم بالوصول:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
cn=config '(olcAccess=*)' olcAccess olcSuffix
```

هنالك المزيد من الأمور التي يجب الحديث عنها في موضوع التحكم في الوصول؛ راجع صفحة الدليل man slapd.access.

ح. TLS

عند الاستيثاق لخادوم OpenLDAP فمن الأفضل استخدام جلسة مشفرة؛ ويمكن أن يتم ذلك باستخدام أمن طبقة النقل (Transport Layer Security [TLS]).

هنا، سنكون «سلطة الشهادة» (Certificate Authority) الخاصة بنا وبعدها سنُنشِئ ونوقع شهادة خادوم LDAP؛ ولما كان slapd مُصَرَّفًا بمكتبة gnutls، فسنستخدم الأداة certtool لإكمال هذه المهام.

١. ثبت حزمتَيّ gnutls-bin و ssl-cert:

```
sudo apt-get install gnutls-bin ssl-cert
```

٢. أنشِئ مفتاحًا خاصًا لسلطة الشهادة:

```
sudo sh -c "certtool \
--generate-privkey > /etc/ssl/private/cakey.pem"
```

٣. أنشئ الملف/القالب /etc/ssl/ca.info لتعريف سلطة الشهادة:

```
cn = Example Company
ca
cert_signing_key
```

٤. أنشِئ شهادة سلطة شهادات موقعة ذاتيًا:

```
sudo certtool --generate-self-signed \
--load-privkey /etc/ssl/private/cakey.pem \
--template /etc/ssl/ca.info \
--outfile /etc/ssl/certs/cacert.pem
```

٥. اصنع مفتاحًا خاصًا للخادوم:

```
sudo certtool --generate-privkey \
--bits 1024 \
--outfile /etc/ssl/private/ldap01_slapd_key.pem
```

ملاحظة: استبدل ldap01 في اسم الملف باسم مضيف خادومك؛ ستساعدك تسمية الشهادة والمفتاح للمضيف والخدمة التي تستخدمها في توضيح الأمور.

٦. أنشئ ملف المعلومات /etc/ssl/ldap01.info الذي يحتوي:

```
organization = Example Company
cn = ldap01.example.com
tls_www_server
encryption_key
signing_key
expiration_days = 3650
```

الشهادة السابقة صالحة لعشرة أعوام، عدِّل هذه القيمة وفقًا لمتطلباتك.

٧. أنشِئ شهادة الخادوم:

```
sudo certtool --generate-certificate \
--load-privkey /etc/ssl/private/ldap01_slapd_key.pem \
--load-ca-certificate /etc/ssl/certs/cacert.pem \
--load-ca-privkey /etc/ssl/private/cakey.pem \
--template /etc/ssl/ldap01.info \
--outfile /etc/ssl/certs/ldap01_slapd_cert.pem
```

أنشئ الملف certinfo.ldif بالمحتويات الآتية (عدلها وفقًا لمتطلباتك؛ حيث اعتبرت أمثلتنا أن الشهادات مُنشَأة باستخدام https://www.cacert.org):

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/cacert.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/ldap01_slapd_cert.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/ldap01_slapd_key.pem
```

استخدم الأمر ldapmodify لإخبار slapd عن عمل TLS عبر قاعدة بيانات slapd-config:

```
sudo ldapmodify -Y EXTERNAL \
-H ldapi:/// -f /etc/ssl/certinfo.ldif
```

وعلى نقيض الاعتقاد الشائع؛ لا تحتاج إلى استخدام //:ldaps في etc/default/slapd/ لكي تستخدم التشفير، كل ما عليك امتلاكه هو:

```
SLAPD_SERVICES="ldap:/// ldapi:///"
```

ملاحظة: أصبح LDAP عبر TLS/SSL (//:dlaps) مهجورًا لتفضيل StartTLS، يشير الأخير إلى جلسة LDAP (تستمع على منفذ TCP ذي الرقم ٣٨٩) التي تصبح محميةً بواسطة TLS/SSl؛ حيث LDAPS -مثل HTTPS- هو بروتوكول منفصل مشفر منذ البداية (encrypted-from-the-start) الذي يعمل على منفذ TCP ذي الرقم ٦٣٦.

اضبط الملكية والأذونات:

```
sudo adduser openldap ssl-cert
sudo chgrp ssl-cert /etc/ssl/private/ldap01_slapd_key.pem
sudo chmod g+r /etc/ssl/private/ldap01_slapd_key.pem
sudo chmod o-r /etc/ssl/private/ldap01_slapd_key.pem
```

أعد تشغيل خدمة OpenLDAP:

```
sudo service slapd restart
```

تحقق من سجلات المضيف (/var/log/syslog) لترى إن بدأ تشغيل الخادوم بنجاح.

ط. التناسخ و TLS

إذا ضبَطت التناسخ بين الخواديم، فمن الممارسات الشائعة هي تشفير (StartTLS) بيانات النسخ المارة في الشبكة لتفادي التنصت عليها؛ وهذا منفصل عن استخدام التشفير والاستيثاق كما فعلنا سابقًا؛ سنبني في هذا القسم على استيثاق TLS.

سنفترض هنا أنك ضبطت الاستنساخ بين المزود والمستهلك وفقًا للقسم «التناسخ»؛ وضبطت TLS للاستيثاق في المزود وفقًا للقسم «TLS».

وكما ذكر سابقًا؛ هدف التناسخ (بالنسبة لنا) هو أن تكون خدمة LDAP ذات إتاحية كبيرةً؛ ولمّا كنا نستخدم TLS للاستيثاق في المزود فإننا نحتاج إلى نفس الأمر في المستهلك؛ بالإضافة إلى ذلك، نريد أن تكون بيانات الاستنساخ المنقولة مشفرةً، وما بقي ليُفعَل هو إنشاء مفتاح وشهادة للمستهلك ثم الضبط وفقًا لذلك، وسنولد المفتاح/الشهادة في المزود؛ لكي نتجنب إنشاء شهادة أخرى لسلطة الشهادات، ثم سننقل ما يلزمنا إلى المستهلك.

في المزود:

أنشِئ مجلدًا (الذي سيستخدم في النقل النهائي)، ثم ولِّد مفتاح المستهلك الخاص:

```
mkdir ldap02-ssl
cd ldap02-ssl
sudo certtool --generate-privkey \
--bits 1024 \
--outfile ldap02_slapd_key.pem
```

أنشئ ملف المعلومات ldap02.info للخادوم المستهلك، وعدِّل قيمه وفقًا لمتطلباتك:

```
organization = Example Company
cn = ldap02.example.com
tls_www_server
encryption_key
signing_key
expiration_days = 3650
```

أنشِئ شهادة المستهلك:

```
sudo certtool --generate-certificate \
--load-privkey ldap02_slapd_key.pem \
--load-ca-certificate /etc/ssl/certs/cacert.pem \
--load-ca-privkey /etc/ssl/private/cakey.pem \
--template ldap02.info \
--outfile ldap02_slapd_cert.pem
```

احصل على نسخة من شهادة سلطة الشهادات:

```
cp /etc/ssl/certs/cacert.pem .
```

لقد انتهينا الآن، انقل مجلد ldap02-ssl إلى المستهلك؛ حيث استخدمنا هنا scp (عدّل الأمر وفقًا لمتطلباتك):

```
cd ..
scp -r ldap02-ssl user@consumer:
```

في المستهلك:

ضبط استيثاق TLS:

```
sudo apt-get install ssl-cert
sudo adduser openldap ssl-cert
sudo cp ldap02_slapd_cert.pem cacert.pem /etc/ssl/certs
sudo cp ldap02_slapd_key.pem /etc/ssl/private
sudo chgrp ssl-cert /etc/ssl/private/ldap02_slapd_key.pem
sudo chmod g+r /etc/ssl/private/ldap02_slapd_key.pem
sudo chmod o-r /etc/ssl/private/ldap02_slapd_key.pem
```

أنشئ الملف /etc/ssl/certinfo.ldif وفيه المحتويات الآتية (عدِّلها وفقًا لمتطلباتك):

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/cacert.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/ldap02_slapd_cert.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/ldap02_slapd_key.pem
```

اضبط قاعدة بيانات slapd-config:

```
sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f certinfo.ldif
```

اضبط /etc/default/slapd في المزود (SLAPD_SERVICES).

في المستهلك:

اضبط TLS للتناسخ من جهة المستهلك، وعدِّل خاصية olcSyncrepl الموجودة مسبقًا بتتبع بعض خيارات TLS؛ وبفعل ذلك، سنرى للمرة الأولى كيف نعدل قيمة خاصية ما.

أنشئ الملف consumer_sync_tls.ldif بالمحتويات الآتية:

```
dn: olcDatabase={1}hdb,cn=config
replace: olcSyncRepl
olcSyncRepl: rid=0 provider=ldap://ldap01.example.com
bindmethod=simple
  binddn="cn=admin,dc=example,dc=com" credentials=secret
searchbase="dc=example,dc=com"
  logbase="cn=accesslog"
logfilter="(&(objectClass=auditWriteObject)(reqResult=0))"
  schemachecking=on type=refreshAndPersist retry="60 +"
syncdata=accesslog
  starttls=critical tls_reqcert=demand
```

الخيارات الإضافية تحدد، على التوالي وبالترتيب، أن على المستهلك استخدام StartTLS وأن شهادة CA مطلوبةٌ للتحقق من هوية المزود، ولاحظ أيضًا صيغة LDIF لتعديل قيم خاصية ما ('replace').

نفِّذ هذه التعديلات:

```
sudo ldapmodify -Y EXTERNAL \
-H ldapi:/// -f consumer_sync_tls.ldif
```

ثم أعد تشغيل slapd:

```
sudo service slapd restart
```

على المزود:

تأكد من أن جلسة TLS قد بدأت؛ وذلك عبر السجل /var/log/syslog، بافتراض أنك أعدت مستوى التسجيل إلى 'conns'، وعليه سترى رسائل شبيهة بالآتي:

```
slapd[3620]: conn=1047 fd=20 ACCEPT from
IP=10.153.107.229:57922 (IP=0.0.0.0:389)
slapd[3620]: conn=1047 op=0 EXT oid=1.3.6.1.4.1.1466.20037
slapd[3620]: conn=1047 op=0 STARTTLS
slapd[3620]: conn=1047 op=0 RESULT oid= err=0 text=
slapd[3620]: conn=1047 fd=20 TLS established tls_ssf=128
ssf=128
slapd[3620]: conn=1047 op=1 BIND
dn="cn=admin,dc=example,dc=com" method=128
slapd[3620]: conn=1047 op=1 BIND
dn="cn=admin,dc=example,dc=com" mech=SIMPLE ssf=0
slapd[3620]: conn=1047 op=1 RESULT tag=97 err=0 text
```

ي. استيثاق LDAP

بعد أن أصبح عندك خادوم LDAP يعمل جيدًا، فستحتاج إلى تثبيت مكتبات على جهاز العميل التي تعلم كيف ومتى عليها أن تتصل إلى الخادوم؛ يتم ذلك في أوبنتو تقليديًا بتثبيت حزمة libnss-ldap؛ ستجلب هذه الحزمة أدواتٍ أخرى، وستساعدك في خطوة الضبط؛ ثبت الآن الحزمة:

```
sudo apt-get install libnss-ldap
```

ستُسأل عن معلوماتٍ حول خادوم LDAP؛ إذا ارتكبت خطأً هنا، يمكنك المحاولة مرة أخرى بالأمر:

```
sudo dpkg-reconfigure ldap-auth-config
```

ستظهر نتائج مربع الحوار السابق في ملف /etc/ldap.conf، إذا تطلّب الخادوم خياراتٍ غير موجودة في القائمة، فعليك تعديل هذا الملف وفقًا لها.

اضبط LDAP لاستخدامه مع NSS:

```
sudo auth-client-config -t nss -p lac_ldap
```

اضبط النظام لاستخدام LDAP للاستيثاق:

```
sudo pam-auth-update
```

اختر LDAP وأيّة آليات استيثاق أخرى قد تحتاج لها من القائمة.

تستطيع الآن تسجيل الدخول بتصاريح مبنية على LDAP.

سيحتاج عملاء LDAP إلى الإشارة إلى عدّة خواديم إذا أُستخدِم الاستنساخ؛ يجب أن تضع شيئًا شبيهًا بالسطر الآتي في ملف /etc/ldap.conf:

```
uri ldap://ldap01.example.com ldap://ldap02.example.com
```

إذا نَفِذَت مهلة (timeout) الطلب، فسيحاول العميل الوصول إلى المستهلك (ldap02) إذا لم يستجيب المزود (ldap01).

إذا كنت تريد استخدام LDAP لتخزين مستخدمي سامبا، فإن عليك ضبط سامبا ليستوثق عبر LDAP، راجع القسم «استخدام سامبا مع LDAP» لمزيد من المعلومات.

ملاحظة: بديل عن حزمة libnss-ldap هي حزمة libnss-ldapd؛ التي ستجلب معها حزمة nscd الذي قد لا نرغب فيها؛ احذفها ببساطة بعد التثبيت.

ك. إدارة المستخدمين والمجموعات

تأتي حزمة ldap-utils مع أدوات كافية لإدارة الدليل، لكن السلسلة الكبيرة من الإعدادات المطلوبة قد تصعّب استخدامها؛ تحتوي حزمة ldapscripts على سكربتات متعلقة بهذه الأدوات التي يجدها بعض الأشخاص أسهل في الاستخدام.

ثبّت الحزمة:

```
sudo apt-get install ldapscripts
```

ثم عدّل الملف /etc/ldapscripts/ldapscripts.conf حتى يصبح شبيهًا بالآتي:

```
SERVER=localhost
BINDDN='cn=admin,dc=example,dc=com'
BINDPWDFILE="/etc/ldapscripts/ldapscripts.passwd"
SUFFIX='dc=example,dc=com'
GSUFFIX='ou=Groups'
USUFFIX='ou=People'
MSUFFIX='ou=Computers'
GIDSTART=10000
UIDSTART=10000
MIDSTART=10000
```

أنشِئ الآن الملف ldapscripts.passwd لكي يستطيع rootDN الوصول إلى الدليل:

```
sudo sh -c "echo -n 'secret' > \
/etc/ldapscripts/ldapscripts.passwd"
sudo chmod 400 /etc/ldapscripts/ldapscripts.passwd
```

ملاحظة: ضع كلمة المرور الخاصة بمستخدم rootDN بدلًا من «secret».

أصبحت السكربتات جاهزةً لإدارة دليلك؛ هذه بضعة أمثلة حول طريقة استخدامها:

إنشاء مستخدم جديد:

```
sudo ldapadduser george example
```

هذا سيُنشِئ مستخدمًا بمعرِّف george ويضبط مجموعة المستخدم الرئيسية إلى example.

تغيير كلمة مرور المستخدم:

```
sudo ldapsetpasswd george
Changing password for user
uid=george,ou=People,dc=example,dc=com
New Password:
New Password (verify):
```

حذف مستخدم:

```
sudo ldapdeleteuser george
```

إضافة مجموعة:

```
sudo ldapaddgroup qa
```

حذف مجموعة:

```
sudo ldapdeletegroup qa
```

إضافة مستخدم إلى مجموعة:

```
sudo ldapaddusertogroup george qa
```

عليك أن ترى الآن خاصية memberUid لمجموعة qa ذات القيمة george.

إزالة مستخدم من مجموعة:

```
sudo ldapdeleteuserfromgroup george qa
```

يجب أن تزال الآن الخاصية memberUid من المجموعة qa.

يسمح لك سكربت ldapmodifyuser بإضافة أو حذف أو استبدل خاصيات المستخدم؛ يستخدم هذا السكربت البنية العامة لأداة ldapmodify، على سبيل المثال:

```
sudo ldapmodifyuser george
# About to modify the following entry :
dn: uid=george,ou=People,dc=example,dc=com
objectClass: account
objectClass: posixAccount
cn: george
uid: george
uidNumber: 1001
gidNumber: 1001
homeDirectory: /home/george
loginShell: /bin/bash
gecos: george
description: User account
userPassword::
e1NTSEF9eXFsTFcyWlhwWkF1eGUybVdFWHZKRzJVMjFTSG9vcHk=

# Enter your modifications here, end with CTRL-D.
dn: uid=george,ou=People,dc=example,dc=com
replace: gecos
gecos: George Carlin
```

يجب أن يصبح الآن المستخدم gecos باسم «George Carlin».

ميـزة جميلـة مـن ميـزات ldapscripts هـو نظـام القـوالب؛ تسـمح لـك القـوالب بتخصـيص خاصيات المستخدم، والمجموعة، وكائنات الجهاز؛ فعلى سبيل المثال، لتفعيل قالب user، عدِّل الملف /etc/ldapscripts/ldapscripts.conf مغيّرًا:

```
UTEMPLATE="/etc/ldapscripts/ldapadduser.template"
```

هنالـك عينـات عـن القـوالب فـي مجلـد /etc/ldapscripts، انسـخ أو أعـد تسـمية ملـف ldapadduser.template.sample إلى /etc/ldapscripts/ldapadduser.template:

```
sudo cp \
/usr/share/doc/ldapscripts/examples/ldapadduser.template.sample \
/etc/ldapscripts/ldapadduser.template
```

عدِّل القالب الجديد ليضيف الخاصيات التي تريدها؛ سيُنشِئ ما يلي مستخدمين جدد بقيمة inetOrgPerson للخاصية objectClass:

```
dn: uid=<user>,<usuffix>,<suffix>
objectClass: inetOrgPerson
objectClass: posixAccount
cn: <user>
sn: <ask>
uid: <user>
uidNumber: <uid>
gidNumber: <gid>
homeDirectory: <home>
loginShell: <shell>
gecos: <user>
description: User account
title: Employee
```

لاحظ القيمة <ask> المُستخدَمة للخاصية sn؛ وهي ما سيجعل ldapadduser يسألك

عن قيمتها.

هنالك أدوات في هذه الحزمة لم نشرحها هنا، هذه هي قائمةٌ كاملةٌ بها:

```
ldaprenamemachine
ldapadduser
ldapdeleteuserfromgroup
ldapfinger
ldapid
ldapgid
ldapmodifyuser
ldaprenameuser
lsldap
ldapaddusertogroup
ldapsetpasswd
ldapinit
ldapaddgroup
ldapdeletegroup
ldapmodifygroup
ldapdeletemachine
ldaprenamegroup
ldapaddmachine
ldapmodifymachine
ldapsetprimarygroup
ldapdeleteuser
```

ل. النسخ الاحتياطي والاسترجاع

الآن يجب أن يعمل LDAP كما نريده تمامًا، فحان الآن الوقت للتحقق من أن عملنا يمكن أن يُستَرجَع وقت الحاجة.

كل ما نحتاج هو طريقة لنسخ قاعدة بيانات ldap احتياطيًا، وخصوصًا السند الخلفي (backend التي هي cn=config) والواجهة الأمامية (frontend التي هي dc=example,dc=com)؛ إذا كنت ستنسخ هذه القواعد نسخًا احتياطيًا إلى -ولِنَقُل- ‎/export/backup، فإننا سنستخدم slapcat كما هو موضَّح في السكربت الآتي المدعو ‎/usr/local/bin/ldapbackup:

```
#!/bin/bash

BACKUP_PATH=/export/backup
SLAPCAT=/usr/sbin/slapcat

nice ${SLAPCAT} -n 0 > ${BACKUP_PATH}/config.ldif
nice ${SLAPCAT} -n 1 > ${BACKUP_PATH}/example.com.ldif
nice ${SLAPCAT} -n 2 > ${BACKUP_PATH}/access.ldif
chmod 640 ${BACKUP_PATH}/*.ldif
```

ملاحظة: هذه الملفات هي ملفات نصية غير مضغوطة تحتوي كل شيء في قواعد بيانات LDAP بما فيها مخطط الشجرة، وأسماء المستخدمين، وكل كلمات المرور؛ لذلك ربما تفكر في جعل ‎/export/backup قسمًا مشفرًا؛ وحتى كتابة سكربت يشفر هذه الملفات عند إنشائها، وربما تفعل كلا الأمرين، ولكن ذلك متعلقٌ بمتطلبات الأمن في نظامك.

كل ما يلزم الآن هو الحصول على سكربت مهام مجدولة (cron) لتشغيل هذا البرنامج كل فترة زمنية (ترى أنها مناسبة)؛ سيكون ملائمًا للكثيرين جدولة تنفيذ البرنامج مرة واحدة كل يوم؛ لكن قد يحتاج الآخرون إلى مراتٍ أكثر في اليوم؛ هذا مثال عن سكربت cron مدعو ‎/etc/cron.d/ldapbackup، والذي سيعمل كل ليلة في تمام الساعة ٢٢:٤٥:

```
MAILTO=backup-emails@domain.com
45 22 * * * root /usr/local/bin/ldapbackup
```

وبعد إنشاء الملفات، يجب نقلها لخادوم النسخ الاحتياطي.

وعلى فرض أنك أعدت تثبيت ldap، فإن عملية الاسترجاع ستكون شبيهةً بما يلي:

```
sudo service slapd stop
sudo mkdir /var/lib/ldap/accesslog
sudo slapadd -F /etc/ldap/slapd.d -n 0 -l \
/export/backup/config.ldif
sudo slapadd -F /etc/ldap/slapd.d -n 1 -l \
/export/backup/domain.com.ldif
sudo slapadd -F /etc/ldap/slapd.d -n 2 -l \
/export/backup/access.ldif
sudo chown -R openldap:openldap /etc/ldap/slapd.d/
sudo chown -R openldap:openldap /var/lib/ldap/
sudo service slapd start
```

م. مصادر

- المصدر الأساسي هو توثيق www.openldap.org.

- هنالك الكثير من صفحات الدليل للحزمة slapd؛ هذه أهمها آخذين بعين الاعتبار المعلومات المقدمة في هذا الفصل:

```
man slapd
man slapd-config
man slapd.access
man slapo-syncprov
```

- صفحات الدليل الأخرى:

```
man auth-client-config
man pam-auth-update
```

- صفحة ويكي مجتمع أوبنتو «OpenLDAP» تحتوي مجموعةً من الملاحظات.

- كتاب O'Reilly المدعو «LDAP System Administration».

- كتاب Packt المدعو «Mastering OpenLDAP».

٢. استخدام سامبا مع LDAP

يشرح هذا القسم دمج سامبا مع LDAP؛ دور خادوم سامبا هو أن يكون خادومًا قائمًا بحد ذاته، ويوفر دليل LDAP بطاقة الاستيثاق بالإضافة إلى احتواء معلومات حساب المستخدم والمجموعة والجهاز التي يتطلبها سامبا لكي يعمل (في أيٍّ من أدواره الممكنة)؛ المتطلب المسبق هو خادوم OpenLDAP مضبوط مع دليل يمكن استخدامه لطلبيات الاستيثاق؛ راجع القسم «خادوم OpenLDAP» لمزيد من المعلومات حول تحقيق هذا المتطلب؛ وبعد إكمال هذا القسم، عليك تحديد ماذا تريد من سامبا أن يفعل لك، وتضبطه وفقًا لذلك.

ا. تثبيت البرمجيات

هنالك ثلاث حزم مطلوبة لدمج سامبا مع LDAP: حزمة samba، و samba-doc، و smbldap-tools.

وإذا أردنا الدقة، فإن حزمة smbldap-tools ليست مطلوبة، لكن ما لم يكن لديك طريقة أخرى لإدارة قيود سامبا المختلفة (المستخدمين والمجموعات والحواسيب) في LDAP، فعليك تثبيتها.

ثبِّت هذه الحزم الآن:

```
sudo apt-get install samba samba-doc smbldap-tools
```

ب. ضبط LDAP

سنضبط الآن خادوم LDAP لكي يلائم بيانات سامبا، إذ أننا سنجري ثلاث مهمات في هذا القسم:

١. استيراد مخطط (schema).

٢. فهرسة بعض القيود.

٣. إضافة كائنات (objects).

مخطط سامبا

لكي يُستخدَم OpenLDAP كسند خلفي (backend) لسامبا؛ فمنطقيًا يجب أن تَستخدم شجرة معلومات الدليل خاصياتٍ تستطيع وصف بيانات سامبا وصفًا سليمًا؛ و يمكن الحصول على مثل هذه الخاصيات باستخدام مخطط سامبا في LDAP؛ لنفعل ذلك الآن.

ملاحظة: لمزيد من المعلومات حول المخططات وتثبيتهم، راجع القسم «تعديل قاعدة بيانات ضبط slapd».

يمكن العثور على المخطط في حزمة samba-doc التي ثبتناها الآن، لكنها تحتاج إلى أن يُفَكَّ ضغطها وتُنسَخ إلى مجلد /etc/ldap/schema:

```
sudo cp /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz
/etc/ldap/schema
sudo gzip -d /etc/ldap/schema/samba.schema.gz
```

احصل على ملف الضبط schema_convert.conf الذي يحتوي على الأسطر الآتية:

```
include    /etc/ldap/schema/core.schema
include    /etc/ldap/schema/collective.schema
include    /etc/ldap/schema/corba.schema
include    /etc/ldap/schema/cosine.schema
include    /etc/ldap/schema/duaconf.schema
include    /etc/ldap/schema/dyngroup.schema
include    /etc/ldap/schema/inetorgperson.schema
include    /etc/ldap/schema/java.schema
include    /etc/ldap/schema/misc.schema
include    /etc/ldap/schema/nis.schema
include    /etc/ldap/schema/openldap.schema
include    /etc/ldap/schema/ppolicy.schema
include    /etc/ldap/schema/ldapns.schema
include    /etc/ldap/schema/pmi.schema
include    /etc/ldap/schema/samba.schema
```

احصل على مجلد ldif_output لكي يُبقي على المخرجات.

حدد فهرس المخطط:

```
slapcat -f schema_convert.conf -F ldif_output -n 0 | \
grep "samba,cn=schema"
dn: cn={14}samba,cn=schema,cn=config
```

حوِّل المخطط إلى صيغة LDIF:

```
slapcat -f schema_convert.conf -F ldif_output -n0 \
-H ldap:///cn={14}samba,cn=schema,cn=config -l cn=samba.ldif
```

عدِّل ملف cn=samba.ldif المولَّد بحذف معلومات الفهرس حتى تصل إلى:

```
dn: cn=samba,cn=schema,cn=config
...
cn: samba
```

احذف الأسطر في الأسفل:

```
structuralObjectClass: olcSchemaConfig
entryUUID: b53b75ca-083f-102d-9fff-2f64fd123c95
creatorsName: cn=config
createTimestamp: 20080827045234Z
entryCSN: 20080827045234.341425Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20080827045234Z
```

ستختلف قيم خاصياتك.

أضف المخطط الجديد:

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f cn=samba.ldif
```

ولطلب وإظهار المخطط الجديد:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL \
-H ldapi:/// -b cn=schema,cn=config 'cn=*samba*'
```

فهارس سامبا

يعرف الآن slapd عن خاصيات سامبا، لنضبط الآن بعض الفهارس (indices) بناءً عليها؛ فهرسة المدخلات هي طريقة لزيادة الأداء عندما يُجرِي العميل بحثًا مُرشَّحًا على شجرة معلومات الدليل.

أنشِئ الملف samba_indices.ldif بالمحتويات الآتية:

```
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: uidNumber eq
olcDbIndex: gidNumber eq
olcDbIndex: loginShell eq
olcDbIndex: uid eq,pres,sub
olcDbIndex: memberUid eq,pres,sub
olcDbIndex: uniqueMember eq,pres
olcDbIndex: sambaSID eq
olcDbIndex: sambaPrimaryGroupSID eq
olcDbIndex: sambaGroupType eq
olcDbIndex: sambaSIDList eq
olcDbIndex: sambaDomainName eq
olcDbIndex: default sub
```

استخدم الأداة ldapmodify لتحميل الفهارس الجديدة:

```
sudo ldapmodify -Q -Y EXTERNAL \
-H ldapi:/// -f samba_indices.ldif
```

إذا جرى كل شيء على ما يرام، فيجب أن تشاهد الفهارس الجديدة باستخدام ldapsearch:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H \
ldapi:/// -b cn=config olcDatabase={1}hdb olcDbIndex
```

إضافة كائنات LDAP لسامبا

تاليًا، اضبط حزمة smbldap-tools لمطابقة بيئتك؛ تأتي هذه الحزمة مع ملف ضبط سيسأل بعض الأسئلة عن الخيارات الضرورية (اسمه smbldap-config.pl، وكان اسمه فيما مضى configure.pl)؛ لكن هنالك علّة ليست مثبتة لكنه موجودة في الكود المصدري (apt-get source smbldap-tools).

لضبط الحزمة يدويًا، عليك إنشاء وتعديل ملفَيّ /etc/smbldap-tools/smbldap.conf و /etc/smbldap-tools/smbldap_bind.conf.

سيضيف سكربت smbldap-populate كائنات LDAP اللازمة لعمل سامبا؛ من الجيد عادةً أن تأخذ نسخةً احتياطيةً من كامل الدليل باستخدام slapcat:

```
sudo slapcat -l backup.ldif
```

أكمل بإملاء الدليل بعد أخذك لنسخةٍ احتياطيةٍ منه:

```
sudo smbldap-populate
```

تستطيع إنشاء ملف LDIF يحتوي كائنات سامبا الجديدة بتنفيذ الأمر sudo smbldap-populate -e samba.ldif؛ وهذا سيسمح لك بمعاينة التعديلات والتأكد من أن كل شيء صحيح؛ ثم نفّذ السكربت لكن بدون الخيار e-؛ أو تستطيع أخذ ملف LDIF واستيراد بياناته كالمعتاد.

يجب أن يملك دليل LDAP الآن المعلومات الضرورية للاستيثاق من مستخدمي سامبا.

ج. ضبط سامبا

هنالك عـدّة طـرق لضـبط سـامبا، لمزيـد مـن المعلومـات حـول بعـض الإعـدادات الشـهيرة، راجع «الفصل الثامن عشر: سامبا»؛ لتضبط سامبا ليستخدم LDAP، فعدِّل الملف /etc/samba/smb.conf وأزل التعليق قبل معامل passdb backend وأضف بعض معاملات ldap:

```
#   passdb backend = tdbsam

# LDAP Settings
    passdb backend = ldapsam:ldap://hostname
    ldap suffix = dc=example,dc=com
    ldap user suffix = ou=People
    ldap group suffix = ou=Groups
    ldap machine suffix = ou=Computers
    ldap idmap suffix = ou=Idmap
    ldap admin dn = cn=admin,dc=example,dc=com
    ldap ssl = start tls
    ldap passwd sync = yes
...
    add machine script = sudo /usr/sbin/smbldap-useradd -t 0 -w
"%u"
```

عدِّل القيم لتطابق بيئتك.

أعد تشغيل خدمة samba لتفعيل الإعدادات الجديدة:

```
sudo restart smbd
sudo restart nmbd
```

أخبر سامبا الآن عن كلمة مرور rootDN (تلك التي ضُبِطَت أثناء تثبيت حزمة slapd):

```
sudo smbpasswd -w password
```

إذا كان لديك مستخدم LDAP موجود مسبقًا، وأردت تضمينه في سامبا، فستحتاج لإضافة بعض الخاصيات؛ تَفعَل أداة smbpasswd هذا أيضًا (يجب أن يقدر المضيف على رؤية [أو سرد] هؤلاء المستخدمين عبر NSS؛ ثَبِّت واضبط إما libnss-ldapd أو libnss-ldap):

```
sudo smbpasswd -a username
```

سيُطلَب منك إدخال كلمة المرور، وستُعتبَر هي كلمة المرور الجديدة لهذا المستخدم.

لإدارة حسابات المستخدم والمجموعة والجهاز، فاستخدم الأدوات الموفرة من حزمة smbldap-tools؛ هذه بعض الأمثلة:

إضافة مستخدم جديد:

```
sudo smbldap-useradd -a -P username
```

يضيف الخيار ‎-a خاصيات سامبا، ويستدعي الخيار ‎-P الأداة smbldap-passwd بعد إنشاء المستخدم مما يسمح لك بإدخال كلمة مرور لذاك المستخدم.

لإزالة مستخدم:

```
sudo smbldap-userdel username
```

استخدِم الخيار ‎-r في الأمر السابق لحذف مجلد المنزل للمستخدم المحدد.

لإضافة مجموعة:

```
sudo smbldap-groupadd -a groupname
```

وكما في الأمر smbldap-useradd، يضيف الخيار a- خاصيات سامبا.

لإنشاء مستخدم جديد ويكون عضوًا في مجموعة:

```
sudo smbldap-groupmod -m username groupname
```

يمكن أن يضيف الخيار m- أكثر من مستخدم في نفس الوقت بسردهم مفصولًا بينهم بفاصلة.

لحذف مستخدم من مجموعة:

```
sudo smbldap-groupmod -x username groupname
```

لإضافة حساب جهاز في سامبا:

```
sudo smbldap-useradd -t 0 -w username
```

استبدل username باسم محطة العمل (workstation)، يُنشِئ الخيار t 0- حساب جهاز بدون تأخير، بينما يحدد الخيار w- الحساب كحساب جهاز؛ لاحظ أيضًا أن معامل add machine script في /etc/samba/smb.conf قد غُيِّر لكي يستخدم smbldap-useradd.

هذه هي الأدوات في حزمة smbldap-tools التي لم نشرحها هنا:

```
smbldap-groupadd
smbldap-groupdel
smbldap-groupmod
smbldap-groupshow
smbldap-passwd
smbldap-populate
smbldap-useradd
smbldap-userdel
smbldap-userinfo
smbldap-userlist
smbldap-usermod
smbldap-usershow
```

د. مصادر

- للمزيد من المعلومات حول تثبيت وضبط سامبا، راجع «الفصل الثامن عشر: سامبا» من هذا الكتاب.
- هنالك عدّة أماكن وثّق فيها LDAP مع سامبا في «Samba HOWTO Collection».
- على الرغم من أن هذه الصفحة قديمة (٢٠٠٧) لكن صفحة «Linux Samba-OpenLDAP HOWTO» تحتوي ملاحظات مهمة.
- الصفحة الرئيسية «Samba Ubuntu community documentation» فيها مجموعة من الوصلات للمقالات المفيدة.

٣. مقدمة عن Kerberos

إن Kerberos هو نظام استيثاق شبكي مبني على مفهوم الجهة الثالثة الموثوقة؛ الجهتان الأخريتان هما المستخدم والخدمة التي يريد المستخدم أن يستوثق فيها؛ لا يمكن لجميع الخدمات والتطبيقات استخدام Kerberos؛ لكن الخدمات التي تستطيع ذلك تجعله يُقرِّب بيئة الشبكة لتصبح أقرب خطوةً إلى «تسجيل الدخول الموحد» (Single Sign On [SSO]).

يشرح هذا القسم تثبيت وضبط خادوم Kerberos، وبعض الأمثلة عن ضبط العملاء.

ا. لمحة عامة

إذا كنت جديدًا على Kerberos، فهذه بعض المصطلحات التي من الجيد معرفتها قبل إعداد خادوم Kerberos، أغلبها مرتبطةٌ بأشياء قد تعرفها من البيئات الأخرى:

- مبدأ (Principal): يجب أن تُعرَّف أيّة مستخدمين أو حواسيب أو خدمات موفرة من الخواديم كمبادئ Kerberos.
- النماذج (Instances): تستخدم لمبادئ الخدمة ومبادئ الإدارة الخاصة.
- الحقول (Realms): الحقل الفريد للتحكم الذي تم تزويده من عملية تثبيت Kerberos؛ تخيل أن الحقول هي مجال أو مجموعة من المضيفين والمستخدمين الذين ينتمون إليها، ويُصطلَح أن الحقل يجب أن يكون بأحرف كبيرة؛ سيستخدم أوبنتو افتراضيًا عنوان DNS مُحوّلًا إلى أحرفٍ كبيرة (EXAMPLE.COM) اسمًا للحقل.

- مركز توزيع المفاتيح (Key Distribution Center [KDC]): يتكون من ثلاثة أقسام: قاعدة بيانات لكل المبادئ، وخادوم استيثاق، وخادوم منح بطاقات (ticket granting server)؛ يجب أن يكون هنالك مركز توزيع للمفاتيح واحد على الأقل لكل حقل.

- بطاقة منح البطاقات (Ticket Granting Ticket): تُصدَر من خادوم الاستيثاق (Authentication Server [AS])؛ بطاقة منح البطاقات (TGT) مشفرة بكلمة مرور المستخدم الذي يعلمها فقط المستخدم و مركز توزيع المفاتيح (KDC).

- خادوم منح البطاقات (Ticket Granting Server [TGS]): يُصدِر خدمة البطاقات للعملاء عند الطلب.

- البطاقات: تأكيد هوية مبدأين، أحد تلك المبادئ هو المستخدم، والآخر هو الخدمة المطلوبة من المستخدم؛ تؤسس البطاقات مفتاح تشفير ليُستخدَم في الاتصالات الآمنة أثناء جلسة الاستيثاق.

- ملفات Keytab: الملفات المستخرجة من قاعدة بيانات مبادئ مركز توزيع المفاتيح وتحتوي على مفتاح التشفير للخدمة أو المضيف.

ولجمع القطع مع بعضها بعضًا، لدى الحقل مركز توزيع مفاتيح واحد على الأقل -ويفضل أن يكون لديه أكثر من واحد لضمان توفر الخدمة- الذي يحتوي على قاعدة بيانات بالمبادئ، وعندما يُسجِّل مستخدمٌ دخوله إلى منصة العمل المضبوطة لاستخدام استيثاق Kerberos؛ فإن مركز توزيع المفاتيح يصدر بطاقة منح البطاقات (TGT)، وإذا كانت التصاريح التي أعطاها المستخدم

مطابقة، فسيتم الاستيثاق من المستخدم وبإمكانه الآن طلب البطاقات لخدمات Kerberos من خادوم منح البطاقات (TGS)، ستسمح خدمة البطاقات للمستخدم أن يستوثق إلى خدمة دون أن يُدخِل اسم المستخدم أو كلمة المرور.

ب. خادوم Kerberos

التثبيت

لنقاشنا هذا، سننشِئ مجال MIT Kerberos مع الخاصيات الآتية (عدِّلها لتلائم حاجاتك):

- الحقل: EXAMPLE.COM.
- مركز توزيع المفاتيح الرئيسي: kdc01.example.com (192.168.0.1).
- مركز توزيع المفاتيح الثانوي: kdc02.example.com (192.168.0.2).
- مبدأ المستخدم: steve.
- مبدأ المدير: steve/admin.

ملاحظة: من المستحسن -وبشدة- أن تكون معرفات مستخدمين الشبكة الموثوقين في مجال مختلف عن المستخدمين المحليين (لنقل أنه يبدأ من ٥٠٠٠).

قبل تثبيت خادوم Kerberos، فمن الضروري وجود خادوم DNS مضبوط مسبقًا؛ ولما كان حقل Kerberos عرفيًا يستخدم اسم النطاق، فإن هذا القسم يستخدم النطاق EXAMPLE.COM المشروحة طريقة ضبطه في قسم الرئيس الأولي في «الفصل الثامن: خدمة اسم النطاق (DNS)».

Kerberos هو بروتوكول حساس بالنسبة للوقت؛ فلو كان وقت النظام المحلي يختلف بين جهاز العميل وجهاز الخادوم أكثر من خمس دقائق (افتراضيًا)، فلن تستطيع منصة العمل أن تستوثق من العميل. ولتصحيح المشكلة، يجب أن يزامن جميع المضيفين وقتهم بواسطة بروتوكول وقت الشبكة (NTP)؛ للمزيد من المعلومات حول ضبط NTP، راجع القسم «مزامنة الوقت باستخدام بروتوكول NTP».

أول خطوة في ضبط حقل Kerberos هي تثبيت حزمتَيّ krb5-kdc و krb5-admin-server؛ أدخل الأمر الآتي في الطرفية:

```
sudo apt-get install krb5-kdc krb5-admin-server
```

ستُسأل في نهاية التثبيت عن اسم مضيف Kerberos وخواديم Admin -اللذان يمكن أن يكونا نفس الخادوم أو غيره- للحقل (realm).

ملاحظة: افتراضيًا، يُنشأ الحقل من اسم نطاق مركز توزيع المفاتيح.

ثم أنشِئ حقلًا جديدًا باستخدام الأداة kdb5_newrealm:

```
sudo kdb5_newrealm
```

الضبط

تستخدم الأسئلة التي سألوك إياها أثناء التثبيت لضبط ملف /etc/krb5.conf؛ إذا احتجت لتعديل إعدادات مركز توزيع المفتاح (KDC) فعدّل ببساطة الملف وأعد تشغيل عفريت krb5-kdc. إذا احتجت لإعادة ضبط Kerberos من الصفر، ربما لتغير اسم الحقل، فيمكنك ذلك بالأمر:

```
sudo dpkg-reconfigure krb5-kdc
```

بعد أن يعمل KDC عملًا سليمًا، فإنه من الضروري وجود مستخدم مدير (مبدأ المدير). من المستحسن استخدام اسم مستخدم مختلف عن اسم المستخدم الذي تستعمله عادةً. يمكن فعل ذلك عبر الأداة kadmin.local، بإدخال الأمر الآتي في الطرفية:

```
sudo kadmin.local
Authenticating as principal root/admin@EXAMPLE.COM with
password.
kadmin.local: addprinc steve/admin
WARNING: no policy specified for steve/admin@EXAMPLE.COM;
defaulting to no policy
Enter password for principal "steve/admin@EXAMPLE.COM":
Re-enter password for principal "steve/admin@EXAMPLE.COM":
Principal "steve/admin@EXAMPLE.COM" created.
kadmin.local: quit
```

في المثال السابق، يكون steve هو مبدأ، و /admin هو نموذج، و يشير @EXAMPLE.COM إلى الحقل، ويكون مبدأ المستخدم هو steve@EXAMPLE.COM، ويجب أن يحمل امتيازات المستخدم العادي فقط.

ملاحظة: استبدل EXAMPLE.COM و steve بالحقل واسم مستخدم المدير عندك على التوالي.

ثم يحتاج مستخدم المدير الجديد إلى أن يحصل على أذونات قوائم التحكم بالوصول (ACL) الملائمة؛ تُضبَط هذه الأذونات في ملف /etc/krb5kdc/kadm5.acl:

```
steve/admin@EXAMPLE.COM          *
```

يعطي هذا القيد steve/admin القدرة على القيام بأي عملية في جميع المبادئ في الحقل؛ تستطيع ضبط المبادئ بامتيازات أقل؛ والذي يكون ملائمًا إذا احتجت مبدأ مدير يستطيع طاقم العمل المبتدئ استخدامه في عملاء Kerberos؛ راجع صفحة الدليل man kadm5.acl لمزيد من التفاصيل.

أعد الآن تشغيل krb5-admin-server لكي تأخذ قوائم التحكم بالوصول الجديدة مفعولها:

```
sudo service krb5-admin-server restart
```

يمكن اختبار مبدأ المستخدم الجديد باستخدام الأداة kinit:

```
kinit steve/admin
steve/admin@EXAMPLE.COM's Password:
```

بعد إدخال كلمة المرور، فاستخدم klist لعرض معلومات حول بطاقة منح البطاقات (TGT):

```
klist
  Credentials cache:   FILE:/tmp/krb5cc_1000
  Principal:           steve/admin@EXAMPLE.COM
     Issued            Expires             Principal
     Jul 13 17:53:34   Jul 14 03:53:34
     krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

حيث اسم ملف التخزين المؤقت krb5cc_1000 مكون من السابقة krb5cc_ ومعرف المستخدم uid، الذي في هذه الحالة ١٠٠٠؛ ربما تحتاج لإضافة قيد في ملف /etc/hosts من أجل مركز توزيع المفاتيح لكي يستطيع العميل العثور عليه، على سبيل المثال:

```
192.168.0.1       kdc01.example.com         kdc01
```

استبدل 192.168.0.1 بعنوان مركز توزيع المفاتيح؛ هذا يحدث عادة عندما تملك حقل Kerberos يشمل عدّة شبكات مفصولة بموجهات (routers).

أفضل طريقة للسماح للعملاء بتحديد مركز توزيع المفاتيح للحقل هو استخدم سجلات DNS SRV، أضف ما يلي إلى /etc/named/db.example.com:

```
_kerberos._udp.EXAMPLE.COM.       IN SRV  1    0 88
kdc01.example.com.
_kerberos._tcp.EXAMPLE.COM.       IN SRV  1    0 88
kdc01.example.com.
_kerberos._udp.EXAMPLE.COM.       IN SRV  10   0 88
kdc02.example.com.
_kerberos._tcp.EXAMPLE.COM.       IN SRV  10   0 88
kdc02.example.com.
_kerberos-adm._tcp.EXAMPLE.COM.   IN SRV  1    0 749
kdc01.example.com.
_kpasswd._udp.EXAMPLE.COM.        IN SRV  1    0 464
kdc01.example.com.
```

ملاحظة: استبدل EXAMPLE.COM، و kdc01 و kdc02، باسم النطاق، ومركز توزيع المفاتيح الرئيسي، ومركز توزيع المفاتيح الثانوي على التوالي وبالترتيب.

انظر إلى الفصل الثامن لتعليمات تفصيلية حول ضبط DNS. أصبح حقل Kerberos الجديد جاهزًا لاستيثاق العملاء.

ج. مركز توزيع المفاتيح الثانوي

بعد أن حصلت على مركز توزيع المفاتيح (KDC) في شبكتك، فمن المستحسن الحصول على مركز ثانوي في حال لم يكن المركز الرئيسي متوافرًا؛ وأيضًا لو كان عندك عملاء Kerberos في شبكات مختلفة (ربما مفصولة بموجهات تستخدم NAT)، فمن الحكمة وضع مركز توزيع ثانوي في كل شبكة من تلك الشبكات.

أولًا، ثبت الحزم، عندما تسأل عن أسماء Kerberos و Admin server فادخل اسم مركز توزيع المفاتيح الرئيسي:

```
sudo apt-get install krb5-kdc krb5-admin-server
```

بعد أن ثبتت الحزم، أنشِئ مبدأ مضيف KDC، بإدخال الأمر الآتي في الطرفية:

```
kadmin -q "addprinc -randkey host/kdc02.example.com"
```

ملاحظة: بعد تنفيذك لأوامر kadmin فستُسأل عن كلمة مرور username/admin@EXAMPLE.COM.

استخرج ملف Keytab:

```
kadmin -q "ktadd -norandkey \
-k keytab.kdc02 host/kdc02.example.com"
```

يجب أن يكون هنالك ملف keytab.kdc02 في مجلدك الحالي، انقل الملف إلى /etc/krb5.keytab:

```
sudo mv keytab.kdc02 /etc/krb5.keytab
```

ملاحظة: المسار إلى keytab.kdc02 يختلف تبعًا لمجلد العمل الحالي.

تستطيع أيضًا أن تُشكِّل قائمةً بالمبادئ في ملف Keytab؛ مما يفيد في استكشاف الأخطاء؛ استخدم الأداة klist:

```
sudo klist -k /etc/krb5.keytab
```

يشير الخيار k- إلى أن الملف هو ملف keytab.

هنالك حاجة لوجود ملف kpropd.acl في كل مركز لتوزيع المفاتيح الذي يعرض كل مراكز توزيع المفاتيح للحقل؛ على سبيل المثال، أَنشِئ في مركز توزيع المفاتيح الرئيسي والثانوي الملف

```
/etc/krb5kdc/kpropd.acl:
host/kdc01.example.com@EXAMPLE.COM
host/kdc02.example.com@EXAMPLE.COM
```

أنشِئ قاعدة بيانات فارغة في المركز الثانوي:

```
sudo kdb5_util -s create
```

ابدأ الآن عفريت kpropd، الذي يستمع إلى الاتصالات من أداة kprop؛ تستخدم أداة kprop لنقل ملفات التفريغ:

```
sudo kpropd -S
```

من الطرفية في مركز توزيع المفاتيح الرئيسي، أنشئ ملف تفريغ من قاعدة بيانات المبادئ:

```
sudo kdb5_util dump /var/lib/krb5kdc/dump
```

استخرج ملف keytab في مركز توزيع المفاتيح الرئيسي وانقله إلى /etc/krb5.keytab:

```
kadmin -q "ktadd -k keytab.kdc01 host/kdc01.example.com"
sudo mv keytab.kdc01 /etc/krb5.keytab
```

ملاحظة: تأكد من وجود مضيف مرتبط مع kdc01.example.com قبل استخراج Keytab.

استخدم الأداة kprop لدفع التغيرات إلى قاعدة البيانات في KDC الثانوي:

```
sudo kprop -r EXAMPLE.COM \
-f /var/lib/krb5kdc/dump kdc02.example.com
```

ملاحظة: يجب أن تَظهر رسالة SUCCEEDED إذا تمت عملية «النسخ» بنجاح، إذا كانت هنالك رسالة خطأ، فتحقق من /var/log/syslog في مركز توزيع المفاتيح الثانوي لمزيدٍ من المعلومات.

ربما ترغب بإنشاء مهمة مجدولة لتحديث قاعدة البيانات في مركز توزيع المفاتيح الثانوي كل فترة زمنية؛ ما يلي سيدفع التغييرات إلى قاعدة البيانات كل ساعة (لاحظ أن السطر الطويل قد جُزِّء لجزأين لكي يتسع في عرض الصفحة):

```
# m h dom mon dow  command
0 * * * * /usr/sbin/kdb5_util dump /var/lib/krb5kdc/dump &&
↪ /usr/sbin/kprop -r EXAMPLE.COM -f /var/lib/krb5kdc/dump
↪ kdc02.example.com
```

أنشئ ملف stash في المركز الثانوي ليُحفَظ به مفتاح Kerberos الرئيسي (Master Key):

```
sudo kdb5_util stash
```

في النهاية، شغل عفريت krb5-kdc في المركز الثانوي:

```
sudo service krb5-kdc start
```

يجب أن يكون المركز الثانوي قادرًا على إعطاء البطاقات للحقل؛ يمكنك اختبار ذلك بإيقاف عفريت krb5-kdc في المركز الرئيسي؛ ثم استخدام kinit لطلب بطاقة، وإذا جرى كل شيء على ما يرام، فيجب أن تحصل على بطاقة من مركز توزيع المفاتيح الثانوي؛ عدا ذلك، تحقق من /var/log/syslog و /var/log/auth.log في مركز توزيع المفاتيح الثانوي.

د. عميل Kerberos للينُكس

يشرح هذا القسم ضبط نظام لينُكس كعميل Kerberos؛ هذا سيسمح بالوصول إلى أيّة خدمة تستخدم Kerberos بعد أن يستطيع المستخدم تسجيل دخوله إلى النظام.

التثبيت

لكـي يتـم الاسـتيثاق إلـى حقـل Kerberos؛ فـإن حزمتَـيّ krb5-user و libpam-krb5 مطلوبتـان؛ بالإضافة إلى غيرها من الحزم غيـر المطلوبة لكنها تسهل عملك؛ أدخِل الأمر الآتي في مِحَث الطرفية لتثبيت هذه الحزم:

```
sudo apt-get install krb5-user libpam-krb5 libpam-ccreds \
auth-client-config
```

تسمح حزمة auth-client-config بضبط PAM ضبطًا بسيطًا للاستيثاق من مصادر عدّة، وستُخزِّن حزمة libpam-ccreds اعتماديات الاستيثاق مما يسمح لك بتسجيل الدخول في حال لـم يكـن مركـز توزيـع المفاتيـح متاحًـا؛ سـتفيد هـذه الحزمـة الحواسـيب المحمولـة، الـتي يمكـن أن تسـتوثق باسـتخدام Kerberos عنـدما تكـون فـي شـبكة الشـركة، لكنهـا تحتـاج إلـى الوصـول عنـدما تكون خارج الشبكة أيضًا.

الضبط

لضبط العميل، أدخل ما يلي في الطرفية:

```
sudo dpkg-reconfigure krb5-config
```

سيُطلَب منك إدخال اسم حقل Kerberos؛ أيضًا إن لم لديك DNS مضبوط مع سجلات Kerberos SRV؛ فستظهر قائمة تسألك عن اسم مضيف مركز توزيع المفاتيح وخادوم إدارة الحقل.

يضيف dpkg-reconfigure قيودًا إلى ملف /etc/krb5.conf للحقل الخاص بك، يجب أن تحصل على قيود شبيهة بالآتي:

```
[libdefaults]
        default_realm = EXAMPLE.COM
...
[realms]
        EXAMPLE.COM = {
                kdc = 192.168.0.1
                admin_server = 192.168.0.1
        }
```

ملاحظة: إذا ضَبطت uid لكلٍ من مستخدمي شبكتك الموثوقين ليبدأ من ٥٠٠٠؛ كما هو منصوح به في قسم «التثبيت»، فتستطيع عندها أن تخبر pam بأن يستوثق باستخدام مستخدمي Kerberos عندما يكون uid أكبر من ٥٠٠٠:

```
# Kerberos should only be applied to ldap/kerberos users, not local ones.
for i in common-auth common-session common-account common-password; do
 sudo sed -i -r \
 -e 's/pam_krb5.so minimum_uid=1000/pam_krb5.so minimum_uid=5000/' \
 /etc/pam.d/$i
done
```

هذا ما سيتجنب الطلب لكلمات مرور (غير موجودة) لمستخدم موثوق محليًا عند تغيير كلمة المرور باستخدام passwd.

يمكنك اختبار الضبط بطلب بطاقة باستخدام الأداة kinit، على سبيل المثال:

```
kinit steve@EXAMPLE.COM
Password for steve@EXAMPLE.COM:
```

يمكن عرض التفاصيل عند إعطاء بطاقة باستخدام klist:

```
klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: steve@EXAMPLE.COM
Valid starting        Expires               Service principal
07/24/08 05:18:56     07/24/08 15:18:56
krbtgt/EXAMPLE.COM@EXAMPLE.COM
renew until 07/25/08 05:18:57

Kerberos 4 ticket cache: /tmp/tkt1000
klist: You have no tickets cached
```

ثم استخدم auth-client-config لضبط وحدة libpam-krb5 لطلب بطاقة أثناء تسجيل الدخول:

```
sudo auth-client-config -a -p kerberos_example
```

يجب أن تحصل الآن على بطاقة بعد عملية استيثاق ناجحة.

٥. مصادر

- للمزيد من المعلومات حول نسخة MIT من Kerberos، راجع موقع «MIT Kerberos».
- توجد بعض التفاصيل في صفحة ويكي أوبنتو «Kerberos».
- الكتاب من O'Reilly المسمى «Kerberos: The Definitive Guide» هو مرجع ممتاز أثناء ضبط Kerberos.
- تستطيع أيضًا القدوم إلى قناتَيّ ‎#ubuntu-server و ‎#kerberos على خادوم IRC الشهير Freenode إذا كانت لديك أسئلة حول Kerberos.

٤. استخدام Kerberos مع LDAP

لا يستعمل أغلب الناس Kerberos لوحده، فبعد أن يستوثق المستخدم (Kerberos)، فسنحتاج لمعرفة ماذا بإمكانه أن يفعل (تصريح [authorization])؛ وهنا تكون مهمة البرامج مثل LDAP.

قد يكون استنساخ قاعدة مبادئ Kerberos بين خادومين أمرًا معقدًا، ويضيف قاعدة بيانات مستخدم أخرى إلى شبكتك؛ لحسن الحظ، MIT Kerberos مضبوطٌ ليستخدم دليل LDAP كقاعدة بيانات للمبادئ؛ يشرح هذا القسم ضبط خادومَيّ Kerberos الرئيسي والثانوي لاستخدام OpenLDAP لقاعدة بيانات المبادئ.

ملاحظة: الأمثلة هنا تستخدم MIT Kerberos و OpenLDAP.

أ. ضبط OpenLDAP

أولًا، يجب تحميل المخطط الضروري على خادوم OpenLDAP الذي لديه اتصال شبكي مع مركز توزيع المفاتيح الرئيسي والثانوي؛ بقية هذا القسم تفترض أن لديك استنساخ LDAP مضبوط بين خادومين على الأقل؛ للمزيد من المعلومات حول ضبط OpenLDAP راجع القسم «خادوم OpenLDAP».

من المطلوب أيضًا ضبط OpenLDAP من أجل اتصالات TLS و SSL؛ لذلك ستكون جميع البيانات المارة بين خادومي LDAP و KDC مشفرةً؛ راجع القسم «TLS» للتفاصيل.

ملاحظة: cn=admin,cn=config هو المستخدم الذي أنشأناه مع امتياز الكتابة إلى قاعدة بيانات ldap؛ تكون القيمة في كثير من الأحيان هي RootDN، عدِّل قيمته وفقًا للضبط عندك.

لتحميل المخطط على LDAP، فثبِّت الحزمة krb5-kdc-ldap في خادوم LDAP؛ أي أدخِل الأمر الآتي في الطرفية:

```
sudo apt-get install krb5-kdc-ldap
```

ثم استخرج محتويات الملف kerberos.schema.gz:

```
sudo gzip -d /usr/share/doc/krb5-kdc-ldap/kerberos.schema.gz
sudo cp /usr/share/doc/krb5-kdc-ldap/kerberos.schema \
/etc/ldap/schema/
```

يجب أن يضاف مخطط kerberos إلى شجرة cn=config؛ آلية إضافة مخطط جديد إلى slapd مفصلةٌ في قسم «تعديل قاعدة بيانات ضبط slapd».

أولًا، أنشِئ ملف ضبط باسم schema_convert.conf، أو أي اسم آخر ذي معنى، يحتوي على الأسطر الآتية:

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/collective.schema
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/duaconf.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema
include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/kerberos.schema
```

أنشِئ مجلدًا مؤقتًا لاحتواء ملفات LDIF:

```
mkdir /tmp/ldif_output
```

استخدم الآن slapcat لتحويل ملفات المخطط:

```
slapcat -f schema_convert.conf -F /tmp/ldif_output -n0 -s \
"cn={12}kerberos,cn=schema,cn=config" > /tmp/cn\=kerberos.ldif
```

عدِّل اسم الملف والمسار السابق ليُطابِق ما عندك إن كان مختلفًا.

عدِّل الخاصيات الآتية في الملف المولَّد /tmp/cn=kerberos.ldif:

```
dn: cn=kerberos,cn=schema,cn=config
...
cn: kerberos
```

واحذف الأسطر الآتية من نهاية الملف:

```
structuralObjectClass: olcSchemaConfig
entryUUID: 18ccd010-746b-102d-9fbe-3760cca765dc
creatorsName: cn=config
createTimestamp: 20090111203515Z
entryCSN: 20090111203515.326445Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20090111203515Z
```

قد تختلف قيم تلك الخاصيات، لكن تأكد أنها قد حُذِفَت.

حمِّل المخطط الجديد بالأمر ldapadd:

```
ldapadd -x -D cn=admin,cn=config -W -f /tmp/cn=kerberos.ldif
```

أضف فهرسًا لخاصية krb5principalname:

```
ldapmodify -x -D cn=admin,cn=config -W
Enter LDAP Password:
dn: olcDatabase={1}hdb,cn=config
add: olcDbIndex
olcDbIndex: krbPrincipalName eq,pres,sub
modifying entry "olcDatabase={1}hdb,cn=config"
```

وفي النهاية، حدِّث قوائم التحكم في الوصول (ACL):

```
ldapmodify -x -D cn=admin,cn=config -W
Enter LDAP Password:
dn: olcDatabase={1}hdb,cn=config
replace: olcAccess
olcAccess: to
attrs=userPassword,shadowLastChange,krbPrincipalKey by
dn="cn=admin,dc=example,dc=com" write by anonymous auth by self
write by * none
-
add: olcAccess
olcAccess: to dn.base="" by * read
-
add: olcAccess
olcAccess: to * by dn="cn=admin,dc=example,dc=com" write by *
read
modifying entry "olcDatabase={1}hdb,cn=config"
```

هذا كل ما في الأمر، أصبح دليل LDAP جاهزًا لكي يخدم كقاعدة بيانات مبادئ Kerberos.

ب. ضبط مركز توزيع المفاتيح الرئيسي

بعد ضبط OpenLDAP، حان الوقت الآن لضبط مركز توزيع المفاتيح.

أولًا، ثبّت الحزم الضرورية الآتية، بتنفيذ الأمر:

```
sudo apt-get install krb5-kdc krb5-admin-server krb5-kdc-ldap
```

عدّل الآن ملف /etc/krb5.conf بإضافة الخيارات الآتية تحت الأقسام الملائمة لها:

```
[libdefaults]
         default_realm = EXAMPLE.COM
...

[realms]
           EXAMPLE.COM = {
                      kdc = kdc01.example.com
                      kdc = kdc02.example.com
                      admin_server = kdc01.example.com
                      admin_server = kdc02.example.com
                      default_domain = example.com
                      database_module = openldap_ldapconf
           }
...

[domain_realm]
           .example.com = EXAMPLE.COM

...

[dbdefaults]
          ldap_kerberos_container_dn = dc=example,dc=com
```

```
[dbmodules]
          openldap_ldapconf = {
             db_library = kldap
             ldap_kdc_dn = "cn=admin,dc=example,dc=com"
             # this object needs to have read rights on
             # the realm container, principal container and
realm sub-trees
             ldap_kadmind_dn = "cn=admin,dc=example,dc=com"
             # this object needs to have read and write rights
on
             # the realm container, principal container and
realm sub-trees
             ldap_service_password_file =
/etc/krb5kdc/service.keyfile
             ldap_servers = ldaps://ldap01.example.com
ldaps://ldap02.example.com
             ldap_conns_per_server = 5
          }
```

ملاحظة: عدِّل قيم example.com، و dc=example,dc=com، و cn=admin,dc=example,dc=com، و ldap01.example.com للقيم الملائمة للنطاق، وكائن LDAP، وخادوم LDAP لشبكتك.

لاحقًا، استخدم الأداة kdb5_ldap_util لإنشاء الحقل:

```
sudo kdb5_ldap_util -D cn=admin,dc=example,dc=com create \
-subtrees dc=example,dc=com -r EXAMPLE.COM -s \
-H ldap://ldap01.example.com
```

أنشِئ «مخبأً» (stash) لكلمة المرور المستخدم في خادوم LDAP، تستخدم هذه الكلمة من ldap_kdc_dn و ldap_kadmind_dn في ملف /etc/krb5.conf:

```
sudo kdb5_ldap_util -D cn=admin,dc=example,dc=com stashsrvpw \
-f /etc/krb5kdc/service.keyfile cn=admin,dc=example,dc=com
```

انسخ شهادة سلطة الشهادات من خادوم LDAP:

```
scp ldap01:/etc/ssl/certs/cacert.pem .
sudo cp cacert.pem /etc/ssl/certs
```

الآن عدِّل /etc/ldap/ldap.conf ليستخدم الشهادة:

```
TLS_CACERT /etc/ssl/certs/cacert.pem
```

ملاحظة: يجب أن تُنسَخ الشهادة أيضًا إلى مركز توزيع المفاتيح الثانوي، للسماح بالاتصال إلى خواديم LDAP باستخدام LDAPS.

تستطيع الآن إضافة مبادئ Kerberos إلى قاعدة بيانات LDAP، وستُنسَخ إلى بقية خواديم LDAP المضبوطة للاستنساخ. فأدخل ما يليل لإضافة مبدأ باستخدام الأداة kadmin.local:

```
sudo kadmin.local
Authenticating as principal root/admin@EXAMPLE.COM with
password.
kadmin.local: addprinc -x
dn="uid=steve,ou=people,dc=example,dc=com" steve
WARNING: no policy specified for steve@EXAMPLE.COM; defaulting
to no policy
Enter password for principal "steve@EXAMPLE.COM":
Re-enter password for principal "steve@EXAMPLE.COM":
Principal "steve@EXAMPLE.COM" created.
```

يجب أن تكون خاصيات krbPrincipalName، و krbPrincipalKey، و krbLastPwdChange، و krbExtraData مضافةً إلى كائن المستخدم uid=steve, ou=people, dc=example, dc=com؛ استخدم أداتَيّ kinit و klist لاختبار إذا أصدر المستخدم المعين بطاقةً.

ملاحظة: إذا كان كائن المستخدم مُنشأً مسبقًا، فإنه يجب إضافة الخيار "..."=x dn- إلى خاصيات Kerberos؛ لأنه سيُنشأ فيما عدا ذلك كائن مبدأي جديد في شجرة الحقل الفرعية.

ج. ضبط مركز توزيع المفاتيح الثانوي

ضبط مركز توزيع المفاتيح الثانوي لاستخدم LDAP هو شبيه بضبطه لاستخدام قاعدة بيانات Kerberos العادية.

أولًا، ثبت الحزم الضرورية، بتطبيق الأمر الآتي في الطرفية:

```
sudo apt-get install krb5-kdc krb5-admin-server krb5-kdc-ldap
```

عدّل الآن ملف /etc/krb5.conf ليستخدم LDAP:

```
[libdefaults]
            default_realm = EXAMPLE.COM

...

[realms]
            EXAMPLE.COM = {
                      kdc = kdc01.example.com
                      kdc = kdc02.example.com
                      admin_server = kdc01.example.com
                      admin_server = kdc02.example.com
                      default_domain = example.com
                      database_module = openldap_ldapconf
            }

...

[domain_realm]
            .example.com = EXAMPLE.COM

...

[dbdefaults]
        ldap_kerberos_container_dn = dc=example,dc=com

[dbmodules]
```

```
        openldap_ldapconf = {
                db_library = kldap
                ldap_kdc_dn = "cn=admin,dc=example,dc=com"
                # this object needs to have read rights on
                # the realm container, principal container and
realm sub-trees
                ldap_kadmind_dn = "cn=admin,dc=example,dc=com"

                # this object needs to have read and write
rights on
                # the realm container, principal container and
realm sub-trees
                ldap_service_password_file =
/etc/krb5kdc/service.keyfile
                ldap_servers = ldaps://ldap01.example.com
                ldaps://ldap02.example.com
                ldap_conns_per_server = 5
        }
```

أنشِئ مخبأً لكلمة مرور LDAP:

```
sudo kdb5_ldap_util -D cn=admin,dc=example,dc=com stashsrvpw \
-f /etc/krb5kdc/service.keyfile cn=admin,dc=example,dc=com
```

الآن انسخ مخبأ «Master Key» على المركز الرئيسي /etc/krb5kdc/.k5.EXAMPLE.COM إلى مركز توزيع المفاتيح الثانوي؛ تأكد من نسخ الملف عبر اتصال مشفر مثل scp، أو عبر وسيط تخزين فيزيائي.

```
sudo scp /etc/krb5kdc/.k5.EXAMPLE.COM steve@kdc02.example.com:~
sudo mv .k5.EXAMPLE.COM /etc/krb5kdc/
```

ملاحظة: مرةً أخرى، استبدل EXAMPLE.COM باسم الحقل الحقيقي.

وبالعودة إلى المركز الثانوي، أعد تشغيل خادوم ldap فقط:

```
sudo service slapd restart
```

في النهاية، ابدأ عفريت krb5-kdc:

```
sudo service krb5-kdc start
```

تأكد أن خادومَيّ ldap (وبالتالي kerberos) متزامنَين.

تستطيع الآن إكمال استيثاق المستخدمين إن أصبح خادوم LDAP أو Kerberos، أو خادوم LDAP وخادوم Kerberos غير متوفرين.

د. مصادر

- لدى دليل «Kerberos Admin Guide» بعض التفاصيل الإضافية.
- للمزيد من المعلومات حول kdb5_ldap_util راجع صفحة دليل man kdb5_ldap_util.
- مصدر آخر مفيد هو صفحة الدليل man krb5.conf.
- انظر أيضًا لصفحة ويكي أوبنتو: «Kerberos and LDAP».

٥. استخدام SSSD مع Active Directory

يشرح هذا القسم استخدام SSSD للاستيثاق من تسجيلات دخول المستخدم باستخدام Active Directory بطريقة «ad»؛ أما في الإصدارات القديمة من sssd، كان من الممكن أن يتم الاستيثاق بطريقة «ldap»، لكن عندما يتم الاستيثاق باستخدام مايكروسوفت ويندوز Active Directory، فكان من الضروري تثبيت إضافات POSIX AD في المتحكم بالنطاق؛ لكن طريقة «ad» تبسِّط الضبط ولا تتطلب أيّة تغيرات في بنية المتحكم بالنطاق.

ا. الشروط المسبقة والافتراضات والمتطلبات

- نفترض أن لديك Active Directory مضبوط وجاهز للعمل.
- نفترض أن المتحكم بالنطاق يعمل كخادوم DNS.
- نفترض أن المتحكم بالنطاق هو خادوم DNS الرئيسي المحدد في /etc/resolv.conf.
- نفترض أن قيود kerberos_، وldap_ و kpasswd_ ...إلخ. مضبوطة في منطقة DNS.
- نفترض أن الوقت مُزامَنٌ على المتحكم بالنطاق.
- النطاق المستخدم في هذا المثال هو myubuntu.example.com.

ب. التثبيت

يجب تثبيت الحزم krb5-user، و samba، و sssd، و ntp؛ نحتاج إلى تثبيت سامبا حتى لو لم يُقدِّم الخادوم أيّة مشاركات. هنالك حاجة لحقل Kerberos والاسم الكامل أو عنوان IP للمتحكمات بالنطاق.

أدخِل الأمر الآتي لتثبيت تلك الحزم:

```
sudo apt-get install krb5-user samba sssd ntp
```

انظر إلى القسم التالي لطريقة الإجابة عن الأسئلة التي يسألها السكربت المشغَّل بعد تثبيت حزمة krb5-user.

ج. ضبط Kerberos

ستُسأل عند تثبيت حزمة krb5-user عن اسم الحقل (realm name) بأحرفٍ كبيرة؛ وعن خادوم مركز توزيع المفاتيح (أي المتحكم بالنطاق) وعن الخادوم المدير (المتحكم بالنطاق أيضًا في هذا المثال)؛ وهذا ما سيكتب القسمين [realm] و [domain_realm] في ملف /etc/krb5.conf؛ هذه الأقسام ليست ضرورية إن كان الاكتشاف التلقائي للنطاق مفعّلًا، خلا ذلك فكلاهما ضروريٌ.

إذا كان اسم النطاق myubuntu.example.com، فأدخِل اسم الحقل كما يلي: MYUBUNTU.EXAMPLE.COM.

وبشكل اختياري، عدِّل الملف /etc/krb5.conf مضيفًا بعض الخيارات لتحديد مدة صلاحية بطاقة Kerberos (هذه القيم جيدة لتستخدم قيمًا افتراضيةً):

```
[libdefaults]

default_realm = MYUBUNTU.EXAMPLE.COM
ticket_lifetime = 24h #
```

```
renew_lifetime = 7d
```

إذا لـم تُحـدَّد قيمـة default_realm، فربمـا مـن الضـروري تسـجيل الـدخول باسـتخدام «username@domain» بدلًا من «username».

يجـب أن يكـون وقـت النظـام فـي عضـو نطـاق Active Directory متوافقًا مع مـثيله فـي المتحكـم بالنطـاق، وإلا فستفشـل عمليـة الاسـتيثاق باسـتخدام Kerberos؛ فمثلًا، يمكـن أن يُـوفِّر خادوم المتحكم بالنطاق خدمة NTP؛ عدِّل الملف /etc/ntp.conf:

```
server dc.myubuntu.example.com
```

د. ضبط سامبا

يجب أن يُستخدَم سامبا لتوفير خدمات netbois/nmbd المتعلقة بالاستيثاق من Active Directory، حتى وإن لم تُشارَك أيّة ملفات. عدِّل الملف /etc/samba/smb.conf وأضف ما يلي إلى قسم [global]:

```
[global]

workgroup = MYUBUNTU
client signing = yes
client use spnego = yes
kerberos method = secrets and keytab
realm = MYUBUNTU.EXAMPLE.COM
security = ads
```

ملاحظة: بعض المراجع تقول أنه يجب تحديد «password server» وأن يشير إلى المتحكم بالنطاق؛ لكن هذا

ضروريٌ فقط إن لم يُضبَط DNS للعثور على المتحكم بالنطاق؛ حيث يَعرِض سامبا افتراضيًا تحذيرًا إن ضُبِطَ الخيار «password server» مع «security = ads».

ه. ضبط SSSD

لا يوجد ملف ضبط افتراضي أو مثال عن ملف الضبط لملف /etc/sssd/sssd.conf في حزمة sssd؛ فمن الضروري إنشاء واحد؛ ها هو ذا أصغر ملف ضبط يمكن أن يعمل:

```
[sssd]

services = nss, pam
config_file_version = 2
domains = MYUBUNTU.EXAMPLE.COM

[domain/MYUBUNTU.EXAMPLE.COM]
id_provider = ad
access_provider = ad

# Use this if users are being logged in at /.
# This example specifies /home/DOMAIN-FQDN/user as $HOME.
# Use with pam_mkhomedir.so
override_homedir = /home/%d/%u

# Uncomment if the client machine hostname doesn't match
# the computer object on the DC.
# ad_hostname = mymachine.myubuntu.example.com

# Uncomment if DNS SRV resolution is not working
# ad_server = dc.mydomain.example.com

# Uncomment if the AD domain is named differently than the
Samba domain
# ad_domain = MYUBUNTU.EXAMPLE.COM

# Enumeration is discouraged for performance reasons.
# enumerate = true
```

بعد حفظ الملف، فانقل الملكية إلى الجذر، وغيِّر أذونات الملف إلى ٦٠٠:

```
sudo chown root:root /etc/sssd/sssd.conf
sudo chmod 600 /etc/sssd/sssd.conf
```

حيث سيرفض sssd أن يعمل إن لم تكن الملكية أو الأذونات صحيحةً.

و. التأكد من ضبط nsswitch.conf

السكربت الذي يعمل بعد تثبيت حزمة sssd يُجري بعض التعديلات على ملف /etc/nsswitch.conf تلقائيًا؛ حيث يجب أن يكون كما يلي:

```
passwd:     compat sss
group:      compat sss
...
netgroup:   nis sss
sudoers:    files sss
```

ز. تعديل ملف /etc/hosts

أضف اسمًا بديلًا الذي يحدد اسم النطاق الكامل للحاسوب المحلي في ملف /etc/hosts كما يلي:

```
192.168.1.10 myserver myserver.myubuntu.example.com
```

هذا مفيد لاستخدامه مع تحديثات DNS الديناميكية.

ح. الانضمام إلى Active Directory

عليك الآن إعادة تشغيل ntp و samba، وتشغيل sssd:

```
sudo service ntp restart
sudo restart smbd
sudo restart nmbd
sudo start sssd
```

ثم اختبر الضبط بمحاولة الحصول على بطاقة Kerberos:

```
sudo kinit Administrator
```

تحقق من البطاقة باستخدام:

```
sudo klist
```

إذا كانت هنالك بطاقة مع تاريخ انتهاء الصلاحية، فقد حان الوقت للانضمام إلى النطاق:

```
sudo net ads join -k
```

التحذير «No DNS domain configured. Unable to perform DNS Update.» يعني أنه ليس هنالك اسم بديل (أو اسم بديل صحيح) في ملف /etc/hosts، ولا يمكن للنظام توفير الاسم الكامل له؛ فعليك التحقق من الاسم البديل في /etc/hosts كما هو مشروح في قسم «تعديل ملف /etc/hosts» أعلاه.

الرسالة «NT_STATUS_UNSUCCESSFUL» تشير إلى أن الانضمام إلى النطاق قد فشل وأن هنالك شيء ما خاطئ، عليك مراجعة الخطوات السابقة وإصلاح المشكلة قبل الإكمال.

هنالك تحققان آخران اختياريان للتأكد من أن الانضمام إلى النطاق قد نجح؛ لاحظ أنه إذا نجح الانضمام إلى النطاق لكن إذا فشل أحد أو كلا التحققين، فربما عليك الانتظار لدقيقةٍ أو دقيقتين قبل المحاولة مرةً أخرى؛ حيث يبدو أن بعض التغيرات لا تحدث في الوقت الحقيقي.

التحقق الأول:

تحقق من «وحدة التنظيم» (Organizational Unit) لحسابات الحواسيب في Active Directory للتأكد من أن حساب الحاسوب قد أُنشِئ (وحدات التنظيم هي موضوع خارج عن نطاق هذا الكتاب).

التحقق الثاني:

نفِّذ الأمر الآتي لمستخدم AD معيّن (المدير مثلًا):

```
getent passwd username
```

ملاحظة: إذا ضبطت الخاصية «enumerate = ture» في ملف sssd.conf، فإن الأمر getnet passwd دون تمرير اسم مستخدم كوسيط سيَعرض جميع مستخدمي النطاق؛ ربما يكون هذا السلوك مفيدًا للاختبار، لكنه بطيء وغير مستحسن للخواديم الإنتاجية.

ط. اختبار الاستيثاق

يجب أن يكون الآن من الممكن الاستيثاق عبر Active Directory:

```
su - username
```

إذا عَمِلَ الأمر السابق بنجاح، فيجب أن تعمل بقية طرق الاستيثاق (getty، و SSH).

إذا أُنشِئ حساب الحاسوب، مما يشير إلى أن النظام قد انضم إلى النطاق، لكن فشل الاستيثاق؛ فربما من المفيد مراجعة الملف /etc/pam.d و sssdwitch.conf وأيضًا تغيرات الملفات المشروحة آنفًا في هذا القسم.

ي. مجلدات المنزل مع pam_mkhomedir

عند تسجيل الدخول باستخدام حساب مستخدم Active Directory، فمن المحتمل ألّا يكون للمستخدم مجلد منزل، ويمكن حل هذه المشكلة باستخدام pam_mkhomedir.so، حيث سيُنشَأ مجلد المنزل للمستخدم عند تسجيل الدخول؛ عدِّل ملف /etc/pam.d/common-session، وأضف هذا السطر مباشرةً بعد «session required pam_unix.so»:

```
session  required  pam_mkhomedir.so skel=/etc/skel/ umask=0022
```

ملاحظة: قد تحتاج إلى «override_homedir» في ملف sssd.conf للعمل عملًا صحيحًا، تأكد من ضبط تلك الخاصية هناك.

ك. الاستيثاق في سطح مكتب أوبنتو

من الممكن أيضًا الاستيثاق من المستخدمين في سطح مكتب أوبنتو باستخدام حسابات Active Directory؛ لكن لن تظهر أسماء حسابات مستخدمي AD في قائمة الاختيار مع المستخدمين المحليين، لذلك يجب تعديل lightdm؛ وذلك بتحرير الملف /etc/lightdm/lightdm.conf.d/50-unity-greeter.conf وإضافة السطرين الآتيين:

```
greeter-show-manual-login=true
greeter-hide-users=true
```

أعد الإقلاع لإعادة تشغيل lightdm، حيث يمكن الآن تسجيل الدخول باستخدام حساب تابع للنطاق إما بالشكل «username» أو «username/username@domain».

ل. المصادر

- صفحة مشروع SSSD.
- مقالة «DNS Server Configuration guidelines».
- صفحة «Active Directory DNS Zone Entries».
- صفحة «Kerberos config options».

٨

خدمة اسم النطاق

DNS

خدمة اسم النطاق (Domain Name Service) هي خدمة إنترنت تربط بين عناوين IP وأسماء النطاق الكاملة (fully qualified domain names [FQDN])؛ وفي هذه الطريقة، تخفف خدمة DNS من حاجة تذكر عناوين IP. تسمى الحواسيب التي تشغّل خدمة DNS «خواديم الأسماء»، ويأتي أوبنتو مع BIND (Brekley Internet Naming Daemon)، وهو أشهر خدمة لإعداد خادوم أسماء في لينُكس.

ا. التثبيت

أدخِل الأمر الآتي في مِحَث الطرفية لتثبيت خادوم dns:

```
sudo apt-get install bind9
```

حزمة dnsutils مفيدةٌ جدًا في اختبار واستكشاف أخطاء DNS؛ قد تكون هذه الأدوات مثبتةً مسبقًا على نظامك؛ لكن للتأكد من وجودها أو تثبيتها، أدخِل الأمر الآتي:

```
sudo apt-get install dnsutils
```

٢. الضبط

هنالك العديد من الطرق لضبط BIND9؛ لكن بعض أشهر هذه الإعدادات هي خادوم تخزين أسماء (caching nameserver)، الرئيس الأولي (primary master)، والرئيس الثانوي (secondary master).

عند ضبطه كخادوم تخزين أسماء، فسيجد BIND9 جوابًا عن استعلامات الأسماء وسيتذكر الجواب عندما يُطلَب النطاق مرةً أخرى.

عندما يُضبَط كخادوم رئيس أولي، فسيقرأ BIND9 البيانات لنطاق (Zone) في ملف في المضيف ويستوثق لهذا النطاق.

عندما يُضبَط كخادوم رئيس ثانوي؛ فسيحصل BIND9 على بيانات النطاق من خادوم أسماء آخر ويستوثق للنطاق.

ا. لمحة

تُخزَّن ملفات ضبط DNS في المجلد /etc/bind، ملف الضبط الرئيسي لتطبيق bind هو /etc/bind/named.conf.

يُحدِّد سطر include اسمَ الملف الذي يحتوي على خيارات DNS؛ سطر directory في ملف /etc/bind/named.conf.options يخبر DNS أين سيبحث عن الملفات، جميع الملفات التي يستخدمها BIND ستتعلق بهذا المجلد.

يصف ملف etc/bind/db.root/ خواديم الأسماء الرئيسية في العالم؛ تتغير هذه الخواديم مع مرور الوقت، لذلك يجب أن يُحدَّث ملف etc/bind/db.root/ بين الحين والآخر؛ وذلك يتم عادةً في تحديثات حزمة bind9؛ يُعرِّف القسم zone خادومًا رئيسيًا (master server)، وهو مخزن في ملف مذكور في خيار file.

من الممكن ضبط نفس الخادوم ليكون خادوم تخزين أسماء، ورئيس أولي، ورئيس ثانوي؛ ويمكن أن يكون الخادوم «بداية السلطة» (Start of Authority [SOA]) لنطاق واحد، بينما يوفر خدمة ثانوية لنطاق آخر؛ ومع كل هذا فهو يوفر خدمات التخزين للمضيفين على الشبكة المحلية LAN.

ب. خادوم تخزين الأسماء

الضبط الافتراضي هو العمل كخادوم تخزين؛ كل ما هو مطلوب هو ببساطة إضافة عناوين IP لخواديم DNS التي وفرها لك مزود الخدمة ISP؛ ببساطة، أزل التعليقات عن الأسطر الآتية وعدلها في ملف etc/bind/named.conf.options/:

```
forwarders {
        1.2.3.4;
        5.6.7.8;
};
```

ملاحظة: استبدل 1.2.3.4 و 5.6.7.8 بعناوين IP لخواديم الأسماء لديك.

أعد الآن تشغيل خادوم DNS لتفعيل الضبط الجديد، وذلك بتنفيذ الأمر الآتي من مِحَث الطرفية:

```
sudo service bind9 restart
```

راجع القسم «dig» لمزيدٍ من المعلومات حول اختبار خادوم تخزين DNS.

ج. الرئيس الأوّلي

سنضبط في هذا القسم BIND9 كخادوم رئيس أولي للنطاق example.com؛ استبدل example.com باسم نطاقك الكامل.

ملف تمرير المنطقة

لإضافة منطقة DNS إلى BIND9، مما يحول BIND9 إلى خادوم رئيس أولي، فإنَّ أول خطوة هي تعديل ملف /etc/bind/named.conf.local:

```
zone "example.com" {
  type master;
          file "/etc/bind/db.example.com";
};
```

ملاحظة: إذا كان سيستقبل bind تحديثاتٍ تلقائيةً عبر DDNS، فعليك استخدام الملف /var/lib/bind/db.example.com بدلًا من /etc/bind/db.example.com سواءً في الملف السابق أو في أمر النسخ الآتي.

استخدم الآن ملف نطاق موجود مسبقًا كقالب لإنشاء ملف /etc/bind/db.example.com:

```
sudo cp /etc/bind/db.local /etc/bind/db.example.com
```

عدِّل ملف النطاق الجديد /etc/bind/db.example.com مغيّرًا localhost إلى FQDN لخادومك، واترك النقطة الإضافية في النهاية؛ وغيّر 127.0.0.1 إلى عنوان IP لخادوم الأسماء و root.localhost إلى عنوان بريد صالح، لكن باستخدام "." بدلًا من رمز "@" واترك أيضًا النقطة الإضافية في النهاية؛ عدِّل التعليق لكي يبيّن النطاق الخاص بهذا الملف.

أنشئ «سجلًا» (record) للنطاق الأساسي، example.com، وأيضًا أنشِئ سجلًا لخادوم الأسماء، الذي هو في هذا المثال ns.example.com:

```
;
; BIND data file for example.com
;
$TTL       604800
@          IN        SO    example.com. root.example.com. (
                           2                ; Serial
                           604800           ; Refresh
                           86400            ; Retry
                           2419200          ; Expire
                           604800           ; Negative Cache TTL
)
@          IN        A        192.168.1.10;
@          IN        NS       ns.example.com.
@          IN        A        192.168.1.10
@          IN        AAAA     ::1
ns         IN        A        192.168.1.10
```

يجب أن تزيد الرقم التسلسلي (Serial Number) في كل مرة تعدِّل فيها على ملف النطاق؛ إذا عدّلت عدة تغيرات قبل إعادة تشغيل BIND9، فَزِد الرقم التسلسلي مرةً واحدةً فقط.

تستطيع الآن إضافة سجلات DNS في نهاية ملف المنطقة، راجع القسم «أنواع السجلات الشائعة» للتفاصيل.

ملاحظة: يحب العديد من مدراء الأنظمة استخدام تاريخ آخر تعديل كرقم تسلسلي للمنطقة؛ مثل 2012010100 الذي هو yyyymmddss (حيث ss هو الرقم التسلسلي).

بعد أن أجريت تعديلاتك في ملف النطاق؛ فيجب إعادة تشغيل BIND9 لكي تأخذ التعديلات مجراها.

```
sudo service bind9 restart
```

ملف النطاق المعكوس

بعد أن ضبطت النطاق لحل الأسماء إلى عناوين IP، فمن المطلوب أيضًا «نطاق معكوس» (Reverse zone)؛ يسمح النطاق المعكوس لخدمة DNS بحل العناوين إلى أسماء.

عدِّل ملف /etc/bind/named.conf.local وأضف ما يلي:

```
zone "1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192";
};
```

ملاحظة: استبدل ١.١٦٨.١٩٢ بأول ثلاث خانات تستخدمها شبكتك؛ وسَمِّ ملف النطاق

/etc/bind/db.192 تسميةً ملائمةً، حيث يجب أن يُطابِق أول خانة من خانات عنوان الشبكة.

أنشِئ الآن ملف /etc/bind/db.192:

```
sudo cp /etc/bind/db.127 /etc/bind/db.192
```

ثم غيِّر ملف /etc/bind/db.192 معدِّلًا نفس الخيارات في /etc/bind/db.example.com:

```
;
; BIND reverse data file for local 192.168.1.XXX net
;
$TTL      604800
@         IN        SOA       ns.example.com. root.example.com.
(
                                     2    ; Serial
                                604800    ; Refresh
                                 86400    ; Retry
                               2419200    ; Expire
                                604800    ; Negative Cache TTL
);
@          IN        NS        ns.
10         IN        PTR       ns.example.com.
```

يجب أن يُزاد الرقم التسلسلي في النطاق المعكوس في كل مرة يُعدَّل فيها الملف. فلكل سجل A تضبطه في /etc/bind/db.example.com لعنوان مختلف، يجب عليك أن تنشِئ سجل PTR في /etc/bind/db.192.

أعد تشغيل BIND9 بعد إنشاء ملف النطاق المعكوس.

```
sudo service bind9 restart
```

د. الرئيس الثانوي

بعد أن يُضبَط الرئيس الأولي فسنحتاج إلى رئيس ثانوي لكي نحافظ على بقاء النطاق في حال لم يكن الرئيس الأولي متوفرًا.

في البداية، يجب أن يُسمَح بنقل النطاق في الخادوم الرئيس الأولي؛ لذا أضف الخيار allow-transfer إلى قسم النطاق والنطاق المعكوس في ملف /etc/bind/named.conf.local:

```
zone "example.com" {
           type master;
  file "/etc/bind/db.example.com";
           allow-transfer { 192.168.1.11; };
};

zone "1.168.192.in-addr.arpa" {
           type master;
           file "/etc/bind/db.192";
  allow-transfer { 192.168.1.11; };
};
```

ملاحظة: استبدل 192.168.1.11 بعنوان IP لخادوم الأسماء الثانوي.

أعد تشغيل خدمة BIND9 في الرئيس الأولي:

```
sudo service bind9 restart
```

الآن ثبِّت على الرئيس الثانوي الحزمة bind9 بنفس الطريقة التي ثبتتها على الأولي؛ ثم عدِّل ملف /etc/bind/named.conf.local وأضف التعاريف الآتية لنطاقَيّ التمرير والعكس:

```
zone "example.com" {
  type slave;
           file "db.example.com";
           masters { 192.168.1.10; };
};

zone "1.168.192.in-addr.arpa" {
 type slave;
          file "db.192";
          masters { 192.168.1.10; };
};
```

ملاحظة: استبدل 192.168.1.10 بعنوان IP لخادوم الأسماء الأولي.

أعد تشغيل خدمة BIND9 على الخادوم الثانوي:

```
sudo service bind9 restart
```

يجب أن تشاهد في سجل /var/log/syslog شيئًا شبيهًا بما يلي (قُسِّمَت بعض الأسطر لكي تتسع في عرض الصفحة):

```
client 192.168.1.10#39448: received notify for zone
'1.168.192.in-addr.arpa'
zone 1.168.192.in-addr.arpa/IN: Transfer started.
transfer of '100.18.172.in-addr.arpa/IN' from 192.168.1.10#53:
 connected using 192.168.1.11#37531
zone 1.168.192.in-addr.arpa/IN: transferred serial 5
transfer of '100.18.172.in-addr.arpa/IN' from 192.168.1.10#53:
 Transfer completed: 1 messages,
6 records, 212 bytes, 0.002 secs (106000 bytes/sec)
zone 1.168.192.in-addr.arpa/IN: sending notifies (serial 5)

client 192.168.1.10#20329: received notify for zone
'example.com'
zone example.com/IN: Transfer started.
transfer of 'example.com/IN' from 192.168.1.10#53: connected
using 192.168.1.11#38577
zone example.com/IN: transferred serial 5
transfer of 'example.com/IN' from 192.168.1.10#53: Transfer
completed: 1 messages,
8 records, 225 bytes, 0.002 secs (112500 bytes/sec)
```

ملاحظة: تُنقَل المنطقة فقط إذا كان الرقم التسلسلي على الأولي أكبر منه على الثانوي؛ وإذا أردت أن يعلم الرئيس الأولي بتعديلات النطاقات في خواديم DNS الثانوية، فعليك إضافة الخيار also-notify { ipaddress; }; في ملف /etc/bind/named.conf.local.

مثال على إضافة الخيار also-notify إلى ملف /etc/bind/named.conf.local:

```
zone "example.com" {
 type master;
 file "/etc/bind/db.example.com";
 allow-transfer { 192.168.1.11; };
 also-notify { 192.168.1.11; };
 };

zone "1.168.192.in-addr.arpa" {
 type master;
 file "/etc/bind/db.192";
 allow-transfer { 192.168.1.11; };
 also-notify { 192.168.1.11; };
 };
```

ملاحظة: المجلد الافتراضي للنطاقات غير الموثوق منها هو /var/cache/bind؛ يُضبَط هذا المجلد أيضًا في AppArmor ليسمح للعفريت named بالكتابة إليه؛ للمزيد من المعلومات حول AppArmor، راجع «الفصل التاسع: الحماية».

٣. استكشاف الأخطاء وإصلاحها

يشرح هذا القسم الطرق التي تستخدم للمساعدة في تحديد المسبب عندما تحدث المشاكل مع DNS و BIND9.

ا. الاختبار

ملف resolv.conf أول خطوة في اختبار BIND9 هي إضافة عنوان IP لخادوم الأسماء للذي يستبين أسماء المضيفين؛ يجب أن يُضبَّط خادوم الأسماء أيضًا لمضيف آخر للتأكد مرةً أخرى؛ تحقق إن كان الملف /etc/resolv.conf يحتوي على الأسطر الآتية:

```
nameserver 192.168.1.10
nameserver 192.168.1.11
```

خواديم الأسماء التي تستمع على *.127 مسؤولة عن إضافة عناوين IP الخاصة بهم إلى ملف resolv.conf (باستخدام resolveconf)؛ وهذا يتم عبر الملف /etc/default/bind9 بتغيير السطر RESOLVECONF=no إلى RESOLVECONF=yes.

ملاحظة: يجب إضافة عنوان IP لخادوم الأسماء الثانوي في حال لم يكن الخادوم الأولي متوفرًا.

```
dig
```

إذا ثبتت حزمة dnsutils فيمكنك اختبار إعداداتك باستخدام أداة البحث في DNS المسماة dig.

بعد تثبيت BIND9، فاستخدم dig مع بطاقة loopback (أي localhost) للتأكد أنها تستمع على المنفذ ٥٣؛ أدخِل الأمر الآتي في مِحَث الطرفية:

```
dig -x 127.0.0.1
```

يجب أن تُشاهِد أسطرًا شبيهة بالآتي في ناتج الأمر:

```
;; Query time: 1 msec
;; SERVER: 192.168.1.10#53(192.168.1.10)
```

إذا ضَبطَت BIND9 كخادوم تخزين الأسماء، فابحث (dig) عن نطاق خارجي للتحقق من زمن الطلبية:

```
dig ubuntu.com
```

لاحظ وقت الطلبية في نهاية ناتج الأمر السابق:

```
;; Query time: 49 msec
```

بعد استخدام dig مرةً أخرى، يجب أن يتحسن الرقم السابق:

```
;; Query time: 1 msec
ping
```

لشرح كيف تَستخدم التطبيقات DNS لكي يستبين اسم المضيف؛ فسنستخدم الأداة ping لإرسال طلب ICMP echo؛ وذلك بإدخال الأمر الآتي في الطرفية:

```
ping example.com
```

ما سبق سيختبر إن استطاع خادوم الأسماء استبيان الاسم ns.example.com وتحويله إلى عنوان IP؛ يجب أن تشابه مخرجات الأمر السابق ما يلي:

```
PING ns.example.com (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=0.800 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=64 time=0.813 ms
named-checkzone
```

طريقة رائعة لاختبار ملفات النطاقات لديك هي استخدام الأداة المثبتة مع حزمة bind9؛ تسمح هذه الأداة لك بالتأكد من أن الضبط صحيح قبل إعادة تشغيل BIND9 وجعل التغيرات حيةً.

أدخِل الأمر الآتي في الطرفية لاختبار ملف النطاق في مثالنا:

```
named-checkzone example.com /etc/bind/db.example.com
```

إذا كان كل شيءٍ مضبوطًا ضبطًا سليمًا، فستشاهد مخرجاتٍ شبيهةٍ بما يلي:

```
zone example.com/IN: loaded serial 6
OK
```

وبشكل مشابه، أدخل ما يلي لاختبار ملف النطاق العكسي:

```
named-checkzone 1.168.192.in-addr.arpa /etc/bind/db.192
```

يجب أن تكون المخرجات شبيهةً بما يلي:

```
zone 1.168.192.in-addr.arpa/IN: loaded serial 3
OK
```

ملاحظة: سيكون الرقم التسلسلي لملف النطاق عندك مختلفًا عادةً.

ب. التسجيل

لدى BIND9 خيارات كثيرة لضبط التسجيل (logging)؛ هنالك خياران رئيسيان هما الخيار channel الذي يضبط أين سيذهب السجل، والخيار category الذي يحدد ما هي المعلومات التي ستُسجَّل.

إذا لم يُحدَّد ضبطٌ للتسجيل، فالضبط الافتراضي هو:

```
logging {
        category default { default_syslog; default_debug; };
        category unmatched { null; };
};
```

يشرح هذا القسم ضبط BIND9 لإرسال رسائل debug متعلقة بطلبيات DNS إلى ملفٍ منفصل.

سنحتاج أولًا إلى ضبط «قناة» (channel) لتحديد الملف الذي ستُرسَل إليه الرسائل، عدل ملف /etc/bind/named.conf.local، وأضف ما يلي:

```
logging {
     channel query.log {
          file "/var/log/query.log";
          severity debug 3;
     };
};
```

اضبط الآن تصنيفًا لإرسال جميع طلبيات DNS إلى ملف query:

```
logging {
     channel query.log {
          file "/var/log/query.log";
          severity debug 3;
     };
     category queries { query.log; };
};
```

ملاحظة: لاحظ أن الخيار debug يمكن أن يُضبَط من المرحلة ١ إلى ٣؛ وستستخدم المرحلة ١ إذا لم تُحدَّد مرحلة.

ولما كان عفريت named يعمل كمستخدم bind، فيجب إنشاء الملف /var/log/query.log وتغيير ملكيته:

```
sudo touch /var/log/query.log
sudo chown bind /var/log/query.log
```

قبل أن يتمكن العفريت named من الكتابة إلى ملف السجل الجديد، فيجب أن يُحدَّث ضبط AppArmor؛ أولًا، عدِّل ملف /etc/apparmor.d/usr.sbin.named وأضف:

```
/var/log/query.log w,
```

ثم أعد تحميل ملف ضبطه:

```
cat /etc/apparmor.d/usr.sbin.named | sudo apparmor_parser -r
```

للمزيد من المعلومات حول AppArmor، راجع الفصل التاسع.

أعد الآن تشغيل BIND9 لكي تأخذ التغييرات مفعولها:

```
sudo service bind9 restart
```

يجب أن ترى الملف /var/log/query.log ممتلئًا بمعلومات الطلبيات؛ هذا مثال بسيط عن ضبط تسجيل BIND9؛ راجع القسم «المزيد من المعلومات» للمزيد من الخيارات المتقدمة.

٤. المراجع

ا. أنواع السجلات الشائعة

يغطي هذا القسم بعض أنواع سجلات DNS الشائعة.

سجل A: يربط هذا السجل عنوان IP إلى اسم مضيف.

```
www             IN      A           192.168.1.12
```

سجل CNAME: يُستخدَم لإنشاء اسم بديل لسجل موجود مسبقًا، لا يمكنك استخدام سجل CNAME للإشارة إلى سجل CNAME آخر.

```
web             IN      CNAME       www
```

سجل MX: يُستخدَم لتعريف أين يجب أن يُرسَل البريد؛ يجب أن يشير إلى سجل A، وليس سجل CNAME.

```
                IN      MX     1    mail.example.com.
mail            IN      A           192.168.1.13
```

سجل NS: يُستخدَم لتعريف أيّة خواديم تُخَدِّم نسخًا من المنطقة؛ يجب أن يشير إلى سجل A، وليس إلى CNAME؛ هذا مكان تعريف الخادومين الأولى والثانوي.

```
                IN      NS          ns.example.com.
                IN      NS          ns2.example.com.
ns              IN      A           192.168.1.10
ns2             IN      A           192.168.1.11
```

ب. المزيد من المعلومات

- دليل «DNS HOWTO» يشرح الخيارات المتقدمة لضبط BIND9.
- انظر إلى bind9.net للحصول على شرح معمّق لعمل DNS و BIND9.
- كتاب «DNS and BIND» هو كتابٌ شائع أصبح في إصداره الخامس؛ وهنالك أيضًا كتاب «DNS and BIND on IPv6».
- مكان رائع لطلب المساعدة في BIND9 والتعاون مع مجتمع خادوم أوبنتو هو قناة IRC على خادوم «#ubuntu-server» Freenode.
- أيضًا، راجع «BIND Server HOWTO» في ويكي أوبنتو.

٩

الحماية

يجب أن تضع الحماية نصب عينيّك عند تثبيت ونشر واستخدام أي نوع من أنظمة تشغيل الحاسوب؛ وعلى الرغم من أن تثبيتًا حديثًا لأوبنتو هو آمن نسبيًا للاستخدام الفوري على الإنترنت، لكن من المهم أن يكون لديك فهم متوازن لحالة حماية أنظمتك بناءً على طريقة استخدامها بعد «نشرها» (deployment).

يزودك هذا الفصل بلمحة عن المواضيع المرتبطة بالحماية المتعلقة بنسخة خادوم أوبنتو ١٤.٠٤، ويخط الخطوط العريضة للإجراءات التي يمكنك أن تستخدمها لحماية خادومك وشبكتك من أي عدد من التهديدات الأمنية المحتملة.

١. إدارة المستخدمين

إدارة المستخدمين هي جزء جوهري في الحفاظ على نظامٍ آمن؛ تقود الإدارة غير الكفء للمستخدمين والامتيازات عادةً إلى إضعاف أمان النظام؛ وبالتالي من الضروري أن تفهم كيف تحميه باستخدام تقنيات إدارة حسابات المستخدمين.

ا. أين هو حساب الجذر؟

اتخذ مطورو أوبنتو قرارًا واعيًا بتعطيل حساب الجذر الإداري افتراضيًا في جميع حالات تثبيت أوبنتو؛ هذا لا يعني أن حساب الجذر محذوفٌ أو لا يمكن الوصول إليه، حيث أُسنِدَت إليه ببساطة كلمة مرور لا تُطابِق أيّة قيمة؛ أي أنك لا تستطيع الدخول إليه مباشرةً.

لكن بدلًا من ذلك، يُحَثّ المستخدمون أن يستخدموا أداةً باسم sudo لتنفيذ مهام إدارة النظام؛ حيث تسمح sudo لمستخدم موثوق بترقية امتيازاته باستخدام كلمة مروره بدلًا من الحاجة لمعرفة كلمة المرور الخاصة بحساب الجذر. هذه الطريقة البسيطة تعطي المسؤولية لجميع أفعال المستخدم، وتمنح مدير النظام تحكمًا بالأفعال التي يستطيع القيام بها مع امتيازاته الحالية.

إذا أردت تفعيل حساب الجذر لسبب ما، فببساطة أسند كلمة مرور لذاك الحساب:

```
sudo passwd
```

ستطلب منك أداة sudo كلمة مرورك، ثم ستطلب منك توفير كلمة مرور جديدة لحساب الجذر كما هو موضح هنا:

```
[sudo] password for username: (enter your own password)
Enter new UNIX password: (enter a new password for root)
Retype new UNIX password: (repeat new password for root)
passwd: password updated successfully
```

استخدم الأمر passwd بهذه الطريقة لتعطيل كلمة مرور حساب الجذر:

```
sudo passwd -l root
```

لكن إذا أردت تعطيل الحساب نفسه، فاستخدم الأمر الآتي:

```
usermod --expiredate 1
```

تستطيع التعلم أكثر عن sudo بالنظر إلى صفحة الدليل المتعلقة بهذا الأمر:

```
man sudo
```

ينتمي المستخدم الذي أُنشِئ أثناء تثبيت أوبنتو افتراضيًا إلى المجموعة «sudo» المُضافة إلى ملف /etc/sudoers كمستخدم sudo موثوق؛ إذا رغبت بمنح أيّ حساب آخر امتيازات الجذر كاملةً عبر sudo، فأضف ذاك الحساب إلى المجموعة sudo.

ب. إضافة وحذف المستخدمين

عملية إدارة المستخدمين المحليين والمجموعات هي عملية بسيطة ومباشرة ولا تختلف إلا قليلًا بين أغلبية أنظمة تشغيل غنو/لينُكس الأخرى؛ تحث أوبنتو، والتوزيعات المبنية على دبيان، على استخدام الحزمة «adduser» لإدارة الحسابات.

لإضافة حساب مستخدم جديد، استخدم الشكل العام الآتي، وأكمل مع الرسائل التي تطلب منك إعطاء كلمة مرور للحساب، وتعريف بعض الخاصيات مثل الاسم الكامل ورقم الهاتف ...إلخ.

```
sudo adduser username
```

استخدم الأمر الآتي لحذف مستخدم ومجموعته الرئيسية:

```
sudo deluser username
```

لا يؤدي حذف حساب مستخدم إلى حذف مجلد المنزل الموافق له؛ هذا يعود لك إن كنت تريد أو لا تريد حذف المجلد يدويًا أو الإبقاء عليه وفقًا لسياساتك.

تـذكر أن أي مسـتخدم آخـر يُضـاف لاحقًـا بنفـس معرفَـيّ UID/GID للمسـتخدم القـديم سيحصل على وصول كامل لهذا المجلد إذا لم تتخذ الاحتياطات اللازمة.

قد ترغب بتغيير قيم UID/GID إلى قيم أخرى ملائمة أكثر -كحساب الجذر مثلًا- وربما تريد أيضًا نقل المجلد لتفادي التضاربات المستقبلية:

```
sudo chown -R root:root /home/username/
sudo mkdir /home/archived_users/
sudo mv /home/username /home/archived_users/
```

لكي تقفل حساب مستخدم مؤقتًا أو تلغي قفله، فاستخدم الأمر passwd مع الخيارات الموافقة للعملية التي تريد إجراءها كما يلي (على التوالي وبالترتيب):

```
sudo passwd -l username
sudo passwd -u username
```

لإضافة أو حذف مجموعة خاصة، فاستخدم الأمرين الآتيين على التوالي وبالترتيب:

```
sudo addgroup groupname
sudo delgroup groupname
```

استخدم الشكل الآتي من أمر adduser لإضافة مستخدم إلى مجموعة:

```
sudo adduser username groupname
```

ج. أمن حساب المستخدم

عنـدما يُنشـأ مسـتخدمٌ جديـد، فستُنشِـئ الأداة adduser مجلـد منـزل جديـد يظهـر باسـم

‎/home/username، يتشكل ملف الحساب (profile) الافتراضي اعتمادًا على المحتويات الموجودة في مجلد ‎/etc/skel الذي يحتوي على أساسيات ضبط الحساب.

إذا كان سيحتوي خادومك على عدّة مستخدمين، فيجب أن تولي أذونات مجلد المنزل للمستخدم اهتمامًا شديدًا لتحقيق سرية بياناته؛ افتراضيًّا، مجلدات منزل المستخدم في أوبنتو تُنشَأ بأذونات القراءة والتنفيذ؛ هذا يعني أن كل المستخدمين يستطيعون الوصول والتجول في محتويات مجلدات المنزل للمستخدمين الآخرين، ربما لا يلائم ذلك احتياجات بيئة تشغيل نظامك.

استخدم الأمر الآتي للتأكد من أذونات مجلد المنزل للمستخدمين الحاليين:

```
ls -ld /home/username
```

يُظهِر الناتج الآتي أن مجلد ‎/home/username لديه أذن القراءة لجميع المستخدمين (العالم أو world):

```
drwxr-xr-x 2 username username 4096 2007-10-02 20:03 username
```

تستطيع إزالة أذن القراءة للجميع بتنفيذ الأمر:

```
sudo chmod 0750 /home/username
```

ملاحظة: بعض الأشخاص يميلون لاستخدام الخيار التعاودي (‎-R [recursive]) دومًا دون تمييز الحالات التي يجب استخدامه فيها، الذي يُعدِّل أذونات المجلدات «الأبناء» والملفات التي فيها، لكن هذا ليس ضروريًا، وربما يتسبب ببعض النتائج غير المرغوب بها؛ يكفي تعديل أذونات المجلد «الأب» فقط لمنع المستخدمين غير

المصرَّح لهم بدخول أي شيء داخل هذا المجلد الأب.

طريقة أخرى أكثر فعاليةً هي تعديل ضبط الأذونات الافتراضية العام للأداة adduser عند إنشاء مجلدات المنزل للمستخدمين الجدد؛ عدِّل ببساطة الملف /etc/adduser.conf وغيِّر قيمة المتغير DIR_MODE إلى قيمةٍ مناسبةٍ، حيث ستحصل جميع مجلدات المنزل الجديدة على الأذونات الصحيحة:

```
DIR_MODE=0750
```

بعد تصحيح أذونات المجلد باستخدام إحدى الطرق السابق ذكرها، فتأكد من النتائج بالأمر:

```
ls -ld /home/username
```

النتائج الآتية تُظهِر أنه قد أُزيل إذن القراءة لجميع المستخدمين:

```
drwxr-x--- 2 username username 4096 2007-10-02 20:03 username
```

د. سياسة كلمة المرور

أحد أهم الجوانب في حماية نظامك هو استخدام سياسة قوية لكلمات المرور؛ إذ تتطلب العديد من الاختراقات الأمنية الناجحة استخدام هجمات «القوة القاسية» (brute force) وتخمين كلمات المرور الضعيفة من القاموس؛ إذا كنت تنوي توفير أي نوع من التحكم البعيد الذي يتطلب كلمة المرور المحلية للنظام، فتأكد أنك تحقق المتطلبات الدنيا من تعقيد كلمات المرور، ومدة كلمة المرور الدنيا، والتدقيق الرتيب لأنظمة الاستيثاق عندك.

طول كلمة المرور الدنيا

تتطلب أوبنتو افتراضيًا طولًا أصغريًا لكلمة المرور يساوي ستة محارف، يمكن التحكم بهذه القيمة في ملف /etc/pam.d/common-password الظاهر هنا:

```
password      [success=2 default=ignore]      pam_unix.so
obscure sha512
```

إذا أردت تغيير الحد الأدنى لطول كلمة المرور إلى ثمانية محارف، فعدِّل المتغير الملائم إلى min=8؛ كما يلي:

```
password      [success=2 default=ignore]      pam_unix.so
obscure sha512 min=8
```

ملاحظة: التحقق البسيط من كلمة المرور، والطول الأدنى لها لا يُطبَّق على الأوامر المُنفَّذة باستخدام sudo لإعداد مستخدم جديد.

مدة صلاحية كلمة المرور

عند إنشاء حسابات للمستخدمين، فيجب أن تُنشِئ سياسة لعمر كلمة المرور الأدنى والأقصى وإجبار المستخدمين على تغيير كلمات مرورهم عندما تنتهي مدتها.

استخدم الأمر الآتي لعرض حالة حساب مستخدم:

```
sudo chage -l username
```

يُظهِر ناتج الأمر السابق حقائق مثيرة للاهتمام حول حساب المستخدم، ولنفترض أنه لا توجد أيّة سياسات مطبَّقة:

```
Last password change                                    : Jan 20, 2008
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires: 7
```

استخدم الأمر الآتي ببساطة وتابع مع الرسائل التفاعلية لضبط أيّة قيمة من هذه القيم:

```
sudo chage username
```

ما يلي مثالٌ لطريقة تغيير تاريخ انتهاء الصلاحية (E-) إلى 01/31/2008، والعمر الأدنى لكلمة المرور (m-) إلى ٥ أيام، والعمر الأقصى لكلمة المرور (M-) إلى ٩٠ يومًا، ومدة الخمول (inactivity، الخيار I-) إلى ٥ أيام بعد انتهاء صلاحية كلمة المرور، ومدة وقت التحذير (W-) إلى ١٤ يومًا قبل انتهاء صلاحية كلمة المرور.

```
sudo chage -E 01/31/2008 -m 5 -M 90 -I 5 -W 14 username
```

للتأكد من التعديلات، استخدم نفس الأمر المذكور آنفًا:

```
sudo chage -l username
```

يجب أن يُظهِر الناتج السياسات الجديدة التي أعددناها لهذا الحساب:

```
Last password change                                    : Jan 20, 2008
Password expires                                        : Apr 19, 2008
Password inactive                                       : May 19, 2008
Account expires                                         : Jan 31, 2008
Minimum number of days between password change          : 5
Maximum number of days between password change          : 90
Number of days of warning before password expires: 14
```

٥. اعتبارات أمنية أخرى

تستخدم العديد من التطبيقات آليات استيثاق أخرى يمكن أن يغفلها حتى مدراء الأنظمة الخبراء؛ وبالتالي فمن المهم فهم والتحكم في طريقة استيثاق المستخدمين وحصولهم على الوصول إلى الخدمات والتطبيقات على خادومك.

وصول SSH من المستخدمين المعطلين

لا يمنع تعطيل حساب مستخدم من دخوله إلى خادومك عن بعد إن كان قد ضبط استيثاق بمفتاح RSA عام؛ وسيتمكنون من الحصول على وصول إلى الصدفة (shell) في الخادوم دون الحاجة لأيّة كلمة مرور؛ تذكر أن تتحقق من مجلد المنزل للمستخدمين الذي يسمحون بهذا النوع من وصول SSH الذي تم الاستيثاق منه؛ أي /home/username/.ssh/authroized_keys.

احذف أو أعد تسمية مجلد ssh/. في مجلد المنزل للمستخدم لتعطيل إمكانيات الاستيثاق عبر SSH.

تأكد أن تتحقق من أيّة اتصالات SSH قد أُنشِئت من المستخدم المعطَّل؛ حيث من الممكن أن يملكوا اتصالات داخلة أو خارجة موجودة مسبقًا، «اقتل» (kill) تلك العمليات إذا عثرت عليها.

```
who | grep username      # to get the pts/X terminal
sudo pkill -f pts/X
```

احصر الوصول عبر SSH إلى حسابات المستخدمين الذين يجب أن يحصلوا عليها فقط؛ فعلى سبيل المثال، ربما تنْشِئ مجموعة تسميها «sshlogin» وتضيف اسم المجموعة كقيمة مرتبطة بالمتغير AllowGroups الموجود في الملف /etc/ssh/sshd_config.

```
AllowGroups sshlogin
```

ثم أضف مستخدمي SSH المسموح لهم إلى المجموعة «sshlogin»، وأعد تشغيل خدمة SSH:

```
sudo adduser username sshlogin
sudo service ssh restart
```

استيثاق المستخدم بقواعد البيانات الخارجية

تتطلب معظم الشبكات المشاريع التجارية آليةَ استيثاقٍ مركزية والتحكم بالوصول إلى جميع مصادر النظام، إذا ضبطت خادومك ليستوثق من المستخدمين من قاعدة بيانات خارجية؛ فتأكد من تعطيل حسابات المستخدمين محليًا وخارجيًا، وبهذا تتأكد من أن البديل المحلي للاستيثاق غير متوفر.

٢. تأمين الطرفية

وكما غيرها من ترسانة الحماية التي تستخدمها لحماية خادومك، من القواعد الصارمة هو التأمين ضد الأضرار الناتجة عن شخص لديه الوصول الفيزيائي لبيئتك، على سبيل المثال، سرقة الأقراص الصلبة، أو خلل في الطاقة الكهربائية ...إلخ؛ وبالتالي يجب أن يكون تأمين الطرفية جزءًا رئيسيًا في استراتيجية الحماية الفيزيائية؛ سيحد «قفل الشاشة» (screen door) من تأثير مجرم عادي، أو على الأقل سيبطئ عمل مجرم مصمم على إلحاق الأذى بنظامك! لذلك من المستحسن إجراء بعض احتياطات الوقاية فيما يتعلق بحماية الطرفية.

سيساعدك ما يلي في الدفاع عن خادومك ضد المشاكل التي قد تسبب عواقب وخيمة.

ا. تعطيل Ctrl+Alt+Delete

بادئ ذي بدء، يستطيع أي شخص لديه الوصول الفيزيائي للوحة المفاتيح ببساطة أن يستخدم تجميعة المفاتيح «Ctrl+Alt+Delete» لإعادة إقلاع الخادوم دون الحاجة لتسجيل الدخول؛ طبعًا يمكن لأي شخص إزالة كبل الكهرباء من المقبس، لكن ما يزال عليك منع استخدام هذه التجميعة على خادوم إنتاجي؛ وهذا يجبر المهاجم على اتخاذ إجراءات عنيفة لإعادة إقلاع الخادوم، وسوف يمنع إعادة الإقلاع غير المقصودة في نفس الوقت.

لتعطيل إعادة إقلاع الخادوم بالضغط على تجميع الأزرار Ctrl+Alt+Delete، فضع رمز التعليق قبل السطر الآتي في ملف /etc/init/control-alt-delete.conf:

```
#exec shutdown -r now "Control-Alt-Delete pressed"
```

٣. الجدار الناري

أ. مقدمة

تتضمن نواة لينُكس النظام الفرعي Netfilter الذي يُستخدَم لتعديل أو تحديد مصير البيانات الشبكية الداخلة أو الخارجة من الخادوم، تَستخدم جميع الجدر النارية في لينُكس هذا النظام لترشيح الرزم الشبكية.

نظام ترشيح الرزم الخاص بالنواة لن يكون مفيدًا لمدراء الأنظمة دون واجهة لإدارته، وهذا هو الغرض من iptables؛ فعندما تصل رزمة شبكية إلى خادومك، فستتوجه إلى النظام الفرعي Netfilter للموافقة أو التعديل أو الرفض بناءً على القواعد الموفَّرة لها من المستخدم عبر iptables؛ ولهذا سيكون iptables هو كل ما تحتاج لإدارة الجدار الناري إن كان مألوفًا لديك، لكن العديد من الواجهات المتوفرة له ستُبسِّط العملية.

ب. الأداة ufw

أداة ضبط الجدار الناري الافتراضية في أوبنتو هي Uncomplicated Firewall أو اختصارًا ufw، التي طُوِّرَت لتسهيل ضبط جدار iptables الناري، توفر ufw واجهة «صديقة» للمستخدم لإنشاء جدار ناري لعناوين IPv4 أو IPv6.

إن ufw معطَّل افتراضيًا. من صفحة دليل man ufw:

«لم يطوَّر ufw لتوفير وظيفة جدار ناري كاملة عبر واجهته السطرية، لكنه يوفر طريقةً سهلةً لإضافة أو حذف القواعد؛ ويستخدم حاليًا استخدامًا رئيسيًا للجدر النارية المعتمدة على المضيف (host-based firewalls).»

هذه بعض أمثلة استخدام ufw:

أولًا، يجب أن نفعِّل ufw، أدخِل الأمر الآتي في الطرفية:

```
sudo ufw enable
```

لفتح منفذ ما (ssh في هذا المثال):

```
sudo ufw allow 22
```

وبشكلٍ مشابه، لإغلاق منفذ مفتوح:

```
sudo ufw deny 22
```

لحذف قاعدة، استخدم الكلمة delete متبوعةً بالقاعدة:

```
sudo ufw delete deny 22
```

من الممكن أيضًا السماح بالوصول من مضيفين أو شبكات محددة لمنفذٍ ما؛ يسمح المثال الآتي بالوصول لمنفذ ssh من المضيف 192.168.0.2 لأي عنوان IP في هذا المضيف:

```
sudo ufw allow proto tcp from 192.168.0.2 to any port 22
```

يمكن استخدام 192.168.0.0/24 بدلًا من 192.168.0.2 للسماح بالوصول عبر ssh لكامل الشبكة الفرعية.

إضافة الخيار dry-run-- لأمر ufw سيجعله يخرج القواعد الناتجة، لكنه لن يطبقها؛ على سبيل المثال، ما يلي هو ما سيحدث لو فتحنا منفذ HTTP:

```
sudo ufw --dry-run allow http

*filter
:ufw-user-input - [0:0]
:ufw-user-output - [0:0]
:ufw-user-forward - [0:0]
:ufw-user-limit - [0:0]
:ufw-user-limit-accept - [0:0]
### RULES ###

### tuple ### allow tcp 80 0.0.0.0/0 any 0.0.0.0/0
-A ufw-user-input -p tcp --dport 80 -j ACCEPT

### END RULES ###
-A ufw-user-input -j RETURN
-A ufw-user-output -j RETURN
-A ufw-user-forward -j RETURN
-A ufw-user-limit -m limit --limit 3/minute -j LOG --log-prefix
"[UFW LIMIT]: "
-A ufw-user-limit -j REJECT
-A ufw-user-limit-accept -j ACCEPT
COMMIT
Rules updated
```

يمكن تعطيل ufw بالأمر:

```
sudo ufw disable
```

أدخل الأمر لمعرفة حالة الجدار الناري:

```
sudo ufw status
```

لمعلومات تفصيلية عن حالة الجدار الناري، استخدم:

```
sudo ufw status verbose
```

لعرض أرقام بجوار القواعد (لحذفها مثلًا) فاستخدم الكلمة المحجوزة numbered:

```
sudo ufw status numbered
```

ملاحظة: إن كان المنفذ الذي تريد فتحه أو إغلاقه معرفًا في /etc/services، فيمكنك استخدام اسم المنفذ بدلًا من رقمه؛ حيث استبدل ٢٢ بالكلمة ssh في الأمثلة السابقة.

هذه مجرد مقدمة سريعة عن استخدام ufw، رجاءً راجع صفحة دليل ufw لمزيد من المعلومات.

دمج التطبيقات مع ufw

تستطيع التطبيقات التي تفتح منافذ أن تُضمِّن ملف ufw الذي يبيّن أيّة منافذ يحتاج التطبيق لفتحها لكي يعمل عملًا تامًا؛ هذه الملفات موجودة في /etc/ufw/applications.d ويمكن أن تُعدَّل إذا تغيَّرت المنافذ الافتراضية.

استخدم الأمر الآتي في الطرفية لعرض التطبيقات التي ثبتت أحد تلك الملفات:

```
sudo ufw app list
```

وبشكل شبيه للسماح بالاتصالات إلى منفذ معين، فيُفعَّل استخدام ملف ضبط أحد التطبيقات بالأمر:

```
sudo ufw allow Samba
```

يمكن استخدام التعبير المُوسَّع كالآتي:

```
ufw allow from 192.168.0.0/24 to any app Samba
```

استبدل «Samba» و 192.168.0.0/24 باسم التطبيق ومجال IP لشبكتك.

ملاحظة: لا توجد هنالك حاجة لتحديد البروتوكول للبرنامج الذي ستُفعِّله، لأن هذه المعلومات مفصَّلة بالملف الخاص به، لاحظ أن اسم التطبيق يستبدل رقم المنفذ.

لعرض معلومات حول المنافذ والبروتوكولات (...إلخ.) المُعرَّفة لتطبيقٍ ما، فأدخِل الأمر:

```
sudo ufw app info Samba
```

ليس لكل التطبيقات التي تتطلب فتح منفذ شبكي ملف ufw خاص؛ إذا كتبت ذاك الملف لتطبيق ما، وأردت أن يُضمَّن هذا الملف مع الحزمة، فرجاءً بلِّغ عن علة في تلك الحزمة على Lanuchpad:

```
ubuntu-bug nameofpackage
```

تنكر IP

الغاية من تنكر IP ‏(IP Masquerading) هو السماح للأجهزة التي تملك IP خاص غير قابل للتوجيه في شبكتك بالوصول إلى الإنترنت عبر الجهاز الذي يقوم بالتنكر؛ يجب أن تُعالَج البيانات الشبكية من شبكتك الخاصة إلى الإنترنت لكي توجَّه الردود إلى الجهاز الذي قام بالطلب، ويجب أن تُعدِّل النواة قيمة عنوان IP المصدر لكل رزمة شبكية لكي تصبح قابلة للتوجيه إلى الخادوم، بدلًا من عنوان IP الخاص (private IP) الذي قام بالطلب، الذي يكون مستحيلًا عبر الإنترنت؛ يستخدم لينُكس تعقب الاتصال (conntrack) لكي يتعقب أيّة اتصالات تتعلق بأيّة أجهزة وإعادة توجيه كل رزمة مُعادة وفقًا لذلك؛ أي أن البيانات الشبكية الخارجة من شبكتك المحلية هي «مُتنكِّرة» لأنها تنشأ من البوابة (خادومك)؛ يُشار إلى هذه العملية في توثيق مايكروسوفت باسم «مشاركة اتصال الإنترنت» (Internet Connection Sharing).

تنكر ufw

يمكن أن يجرى تنكر IP بقواعد ufw مخصصة؛ هذا ممكن لأن السند الخلفي للأداة ufw هو iptables-restore مع ملفات القواعد المخزنة في /etc/ufw/*.rules؛ هذه الملفات هي مكان ممتاز لإضافة قواعد iptables بدون ufw، وللقواعد التي تتعلق تعلقًا كبيرًا بالبوابات الشبكية أو الجسور.

تُقسَّم القواعد إلى ملفين مختلفين، القواعد التي يجب أن تُنَفَّذ قبل القواعد السطرية التابعة للأداة ufw، والقواعد التي تُنفَّذ بعدها.

أولًا، يجب أن يُفعَّل تمرير الرزم في ufw، يجب أن يُعدَّل ملفي إعدادات؛ غيِّر قيمة DEFAULT_FORWARD_POLICY إلى "ACCEPT" في ملف ‎/etc/default/ufw:

```
DEFAULT_FORWARD_POLICY="ACCEPT"
```

ثم عدِّل الملف ‎/etc/ufw/sysctl.conf وأزل التعليق عن:

```
net/ipv4/ip_forward=1
```

وبشكل مشابه، لتمرير IPv6 أزل التعليق عن:

```
net/ipv6/conf/default/forwarding=1
```

سنضيف الآن القواعد إلى ملف ‎/etc/ufw/before.rules؛ القواعد الافتراضية تضبط جدول filter فقط، ويجب ضبط جدول nat لتفعيل التنكر؛ أضف ما يلي إلى أعلى الملف بعد تعليقات الترويسة مباشرةً:

```
# nat Table rules
*nat
:POSTROUTING ACCEPT [0:0]

# Forward traffic from eth1 through eth0.
-A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE

# don't delete the 'COMMIT' line or these nat table rules won't
be processed
COMMIT
```

ليست التعليقات ضروريةً، لكنها من المستحسن توثيق ملفات الضبط؛ وعند تعديل أي من ملفات «القواعد» في /etc/ufw، فتأكد من أن هذين السطرين موجودان في نهاية الملف لكل جدول عدّلته:

```
# don't delete the 'COMMIT' line or these nat table rules won't
be processed
COMMIT
```

يجب أن تتوفر عبارة COMMIT في نهاية كل جدول، وقد ظهر في الأمثلة السابقة جدولًا nat و filter فقط، لكنك تستطيع إضافة القواعد لجدولَيّ raw و mangle.

ملاحظة: استبدل-في المثال السابق- eth0 و eth1 و 192.168.0.0/24 بالبطاقات ومجال IP الملائمين.

في النهاية، عطّل وأعد تفعيل ufw لتطبيق التغيرات:

```
sudo ufw disable && sudo ufw enable
```

يجب أن يُفعَّل تنكر IP الآن، تستطيع إضافة أية قواعد FORWARD إضافية إلى ملف /etc/ufw/before.rules؛ من المستحسن إضافة هذه القواعد في سلسلة ufw-before-forward.

تنكر iptables

يمكن أن يُستخدَم iptables لتفعيل التنكر. وبشكل شبيه للأداة ufw، أول خطوة هي تفعيل تمرير IPv4 بتعديل ملف /etc/sysctl.conf وإزالة التعليق عن السطر الآتي:

```
net.ipv4.ip_forward=1
```

إذا أردت تفعيل تمرير IPv6، فأزل التعليق عن:

```
net.ipv6.conf.default.forwarding=1
```

تاليًا، نفِّذ الأمر sysctl لتفعيل الإعدادات الجديدة في ملف الضبط:

```
sudo sysctl -p
```

يمكن أن يُفعَّل تنكر IP بقاعدة iptables واحدة، التي يمكن أن تختلف اختلافًا بسيطًا بناءً على ضبط شبكتك:

```
sudo iptables -t nat -A POSTROUTING -s 192.168.0.0/16 \
-o ppp0 -j MASQUERADE
```

يفترض الأمر السابق أن مجال شبكتك الخاصة هو 192.168.0.0/16 وأن الجهاز الذي يمتلك اتصالًا بالإنترنت هو ppp0، نستطيع تقسيم الأمر السابق كما يلي:

- ‎-t nat: القاعدة ستذهب لجدول nat.
- ‎-A POSTROUTING: ستُضاف القاعدة (‎-A) إلى سلسلة POSTROUTING.

- 192.168.0.0/16 s-: تطبَّق القاعدة على البيانات الآتية من مجال العناوين المحدد.
- o ppp0-: القاعدة تُطبَّق على البيانات المقرر توجيهها عبر الجهاز الشبكي المحدد.
- j MASQUERADE-: ستقفز (jump) البيانات المُطابِقة لهذه القاعدة إلى هدف MASQUERADE لكي تُعالَج كما هو مشروح في الأعلى.

أيضًا، كل سلسلة في جدول filter (الجدول الافتراضي، ومكان حدوث أغلبية ترشيح الرزم الشبكية) تكون سياستها الافتراضية هي ACCEPT؛ لكن إن كنت تُنشِئ جدارًا ناريًا بالإضافة إلى بوابة، فربما تحتاج إلى ضبط السياسات إلى DROP أو REJECT؛ وفي هذه الحالة تحتاج البيانات المتنكرة إلى السماح لها في سلسلة FORWARD لكي تعمل القاعدة السابقة:

```
sudo iptables -A FORWARD -s 192.168.0.0/16 -o ppp0 -j ACCEPT
sudo iptables -A FORWARD -d 192.168.0.0/16 -m state \
--state ESTABLISHED,RELATED -i ppp0 -j ACCEPT
```

ستسمح الأوامر السابقة لجميع الاتصالات من شبكتك المحلية إلى الإنترنت، ولعودة البيانات المتعلقة بهذه الاتصالات إلى الجهاز الذي طلبها.

إذا أردت تفعيل التنكر عند الإقلاع -الذي تريد تفعيله في غالب الأحيان- فعدِّل ملف /etc/rc.local وأضف الأوامر السابقة؛ على سبيل المثال، أضف الأمر السابق دون ترشيح:

```
iptables -t nat -A POSTROUTING -s 192.168.0.0/16 -o ppp0 \
-j MASQUERADE
```

ج. السجلات

سجلات الجدار الناري مهمة جدًا للتعرف على الهجمات، واستكشاف أخطاء قواعد الجدار الناري، وملاحظة النشاط غير الطبيعي في شبكتك؛ يجب أن تضمِّن قواعد للتسجيل في جدارك الناري لكي تولِّد السجلات، ويجب أن تأتي قواعد السجلات قبل قواعد الإنهاء (القواعد التي تحدد مصير الرزمة، مثل ACCEPT، أو DROP أو REJECT).

إذا كنت تستخدم ufw، فبإمكانك تفعيل التسجيل بإدخال الأمر الآتي في الطرفية:

```
sudo ufw logging on
```

لكي توقف التسجيل في ufw، فببساطة بدل on بالكلمة off في الأمر السابق.

إذا كنت تستخدم iptables بدلًا من ufw، فأدخل الأمر:

```
sudo iptables -A INPUT -m state --state NEW -p tcp \
--dport 80 -j LOG --log-prefix "NEW_HTTP_CONN: "
```

طلبيةٌ على المنفذ ٨٠ من الجهاز المحلي ستولدُ سجلًا في dmesg الذي يبدو كما يلي (سطرٌ واحدٌ فقط قُسِّمَ إلى عدّة أقسام لكي يتسع في عرض الصفحة):

```
[4304885.870000] NEW_HTTP_CONN: IN=lo OUT=
 ↪ MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00
 ↪ SRC=127.0.0.1 DST=127.0.0.1 LEN=60 TOS=0x00 PREC=0x00 TTL=64
 ↪ ID=58288 DF PROTO=TCP SPT=53981 DPT=80 WINDOW=32767 RES=0x00
 ↪ SYN URGP=0
```

سيظهر السجل السابق في ملف /var/log/massages/، و /var/log/syslog/، و كذلك /var/log/kern.log/؛ يمكن تعديل هذا السلوك بتعديل /etc/syslog.conf/ تعديلًا ملائمًا أو بتثبيت وضبط ulogd وباستخدام الهدف ULOG بدلًا من LOG.

العفريت ulogd هو خادوم في مجال المستخدم (userspace server) الذي يستمع إلى تعليمات التسجيل من النواة وخصوصًا للجدر النارية، ويمكنك التسجيل إلى أي ملف تريد، وحتى إلى قواعد بيانات PostgreSQL أو MySQL؛ يمكن تسهيل فهم سجلات الجدار الناري باستخدام أداة تحليل سجلات مثل logwatch، أو fwanalog، أو fwlogwatch، أو lire.

د. أدوات أخرى

هنالك أدوات عديد متوفرة لتساعدك في بناء جدار ناري كامل دون أن تكون لديك المعرفة الجيدة باستخدام iptables؛ للميالين للبرامج الرسومية:

- برنامج fwbulider1 هو قوي جدًا وسيكون مألوفًا للمدراء الذين تعاملوا مع أدوات تجارية لإدارة الجدر النارية، مثل Checkpoint FireWall-1.

إذا كنت تُفضّل أداةً من سطر الأوامر مع ملفات ضبط نصيّة:

- الأداة Shorewall2 هي أداة قوية جدًا لتساعدك في ضبط جدار ناري متقدم لأي شبكة.

٥. مصادر

- صفحة ويكي أوبنتو «Ubuntu Firewall» التي تحتوي على معلومات عن تطوير ufw.
- أيضًا، صفحة دليل ufw تحتوي معلومات مفيدة جدًا: man ufw.
- راجع الصفحة «packet filtering HOWTO» للمزيد حول استخدام iptables.
- صفحة «nat-HOWTO» تحتوي تفاصيل إضافية عن التنكر.
- صفحة ويكي أوبنتو «IPTables HowTo» هي مصدر رائع للمعلومات.

٤. برمجية AppArmor

إن AppArmor هو وحدة حماية في لينُكس تقيّد وصول البرامج المختلفة إلى قائمة بالملفات التابعة لها والإمكانيات المذكورة في مسودة posix 1003.le.

إن AppArmor مثبَّت ومفعَّل افتراضيًا، ويستخدم «ملفات ضبط» (profiles) للتطبيقات لتحديد أيّة ملفات وأذونات يتطلبها التطبيق، بعض الحزم تُثبِّت ملفات الضبط الخاصة بها، ويمكن العثور على ملفات ضبط إضافية في حزمة apparmor-profiles.

أدخل الأمر الآتي في الطرفية لتثبيت حزمة apparmor-profiles

```
sudo apt-get install apparmor-profiles
```

لملفات ضبط AppArmor نمطين من التنفيذ:

- البناء أو التعلم (Complaining/Learning): من المسموح تجاوز ملف الضبط وستُسجَّل تلك التجاوزات؛ يفيد هذا النمط في اختبار وتطوير ملفات ضبط جديدة.
- الإجبار أو التقييد (Enforced/Confined): إجبار السياسة في ملفات الضبط، وتسجيل التجاوزات أيضًا.

ا. استخدام AppArmor

تنويه: هذا القسم معلول بعلّة، فللأسف لن تعمل الأوامر التي فيه كما يجب.

تحتوي حزمة apparmor-utils على أدوات سطر أوامر تمكّنك من تغيير نمط تنفيذ AppArmor، أو معرفة حالة ملف ضبط، أو إنشاء ملفات جديدة ...إلخ.

يُستخدَم الأمر apparmor_status لعرض حالة ملفات ضبط AppArmor.

```
sudo apparmor_status
```

يضع الأمر aa-complain ملفَ ضبطٍ قيدَ البناء:

```
sudo aa-complain /path/to/bin
```

الأمر aa-enforce يضعُ ملفَ ضبطٍ قيدَ التنفيذ:

```
sudo aa-enforce /path/to/bin
```

المجلد ‎/etc/apparmor.d هو مكان تواجد ملفات ضبط AppArmor؛ يمكن أن يُستخدَم لتعديل «نمط» جميع ملفات الضبط.

أدخِل ما يلي لوضع كل الملفات في نمط البناء:

```
sudo aa-complain /etc/apparmor.d/*
```

لوضع جميع الملفات قيد التنفيذ:

```
sudo aa-enforce /etc/apparmor.d/*
```

يُستخدَم الأمر apparmor_parser لتحميل ملف ضبط إلى النواة، ويمكن أن يُستخدَم لإعادة تحميل ملف ضبط مُحمَّل مسبقًا باستخدام الخيار r-؛ لتحميل ملف ضبط:

```
cat /etc/apparmor.d/profile.name | sudo apparmor_parser -a
```

ولإعادة تحميل ملف ضبط محمَّل مسبقًا:

```
cat /etc/apparmor.d/profile.name | sudo apparmor_parser -r
```

يمكن استخدام service apparmor لإعادة تحميل كل ملفات الضبط:

```
sudo service apparmor reload
```

يمكن استخدام المجلد /etc/apparmor.d/disable مع الخيار apparmor_parser - R لتعطيل ملف ضبط:

```
sudo ln -s /etc/apparmor.d/profile.name \
/etc/apparmor.d/disable/
sudo apparmor_parser -R /etc/apparmor.d/profile.name
```

لإعادة تفعيل ملف ضبط معطَّل، احذف الوصلة الرمزية إلى الملف في /etc/apparmor.d/disable ثم أعد تحميل ملف الضبط باستخدام الخيار a-:

```
sudo rm /etc/apparmor.d/disable/profile.name
cat /etc/apparmor.d/profile.name | sudo apparmor_parser -a
```

يمكن تعطيل AppArmor، وسيزال تحميل وحدة النواة بإدخال ما يلي:

```
sudo service apparmor stop
sudo update-rc.d -f apparmor remove
```

لإعادة تفعيل AppArmor، أدخِل:

```
sudo service apparmor start
sudo update-rc.d apparmor defaults
```

ملاحظة: استبدل profile.name باسم ملف الضبط الذي تريد تعديله، أيضًا استبدل /path/to/bin بمسار الملف التنفيذي الحقيقي؛ على سبيل المثال، للأمر ping استخدم /bin/ping.

ب. ملفات الضبط

ملفات الضبط (profiles) هي ملفات نصية بسيطة موجودة في /etc/apparmor.d/؛ هذه الملفات مسماةٌ وفقًا للمسار الكامل للملف التنفيذي الذي تضبطه لكن مع إبدال «/» بنقطة «.»؛ على سبيل المثال، /etc/apparmor.d/bin.ping هو ملف ضبط AppArmor للأمر /bin/ping.

هنالك نوعان رئيسيان من القواعد المستخدمة في ملفات الضبط:

- قيود المسار (Path entries): التي تحدد الملفات التي يمكن للتطبيق الوصول إليها في نظام الملفات.
- قيود الإمكانيات (Capability entries): تحدد الامتيازات المسموحة لعملية مقيدة.

ألقِ نظرةً على /etc/apparmor.d/bin.ping كمثال:

```
#include <tunables/global>
/bin/ping flags=(complain) {
  #include <abstractions/base>
  #include <abstractions/consoles>
  #include <abstractions/nameservice>

  capability net_raw,
  capability setuid,
  network inet raw,

  /bin/ping mixr,
  /etc/modules.conf r,
}
```

- #include <tunables/global>: تضمين تعبيرات من ملفات أخرى، وهذا يسمح للعبارات المشتركة بين عدّة تطبيقات بالتواجد في ملف مشترك.
- /bin/ping flags=(complain): المسار إلى التطبيق صاحب ملف الضبط، وضبط النمط إلى complain.
- capability net_raw,: السماح بالوصول إلى امتياز Posix.le CAP_NET_RAW.
- /bin/ping mixr,: السماح للتطبيق بوصول القراءة والتنفيذ إلى الملف.

ملاحظة: يجب إعادة تحميل ملف الضبط بعد تعديله، راجع القسم «استخدام AppArmor» للتفاصيل.

إنشاء ملف ضبط

صمم خطة اختبار: فكر كيف يمكن «تمرين» التطبيق؛ يجب أن تُقسَّم خطة الاختبار إلى حالات اختبار صغيرة، وكل حالة اختبار لها شرح صغير وقائمة بالخطوات التي يجب اتباعها.

بعض حالات الاختبار القياسية هي:

- بدء تشغيل البرنامج.
- إيقاف البرنامج.
- إعادة تحميل البرنامج.
- اختبار جميع الأوامر المدعومة من سكربت init.

توليد ملف الضبط الجديد: استخدم aa-genprof لتوليد ملف ضبط جديد؛ من الطرفية:

```
sudo aa-genprof exectable
```

على سبيل المثال:

```
sudo aa-genprof slapd
```

لكي يُضمَّن ملف الضبط الجديد الخاص بك في حزمة apparmor-profiles، فبلِّغ عن علة في Lanuchpad عن حزمة AppArmor:

- ضمِّن خطة الاختبار وحالات الاختبار.
- أضف ملف الضبط الجديد إلى العلة.

تحديث ملفات الضبط

عندما لا يعمل برنامج ما كما يجب؛ فافحص الرسائل التي تُرسَل إلى ملفات السجل؛ يمكن أن يُستخدَم البرنامج aa-logprof لفحص ملفات السجل لرسائل التدقيق الخاصة ببرنامج AppArmor؛ راجعها وحدِّث ملفات الضبط.

```
sudo aa-logprof
```

ج. مصادر

- راجع «AppArmor Administraion Guide» لإعدادات الضبط المتقدمة.
- للتفاصيل حول استخدام AppArmor مع إصدارات أخرى من أوبنتو، فراجع صفحة ويكي المجتمع حول AppArmor.
- صفحة «OpenSUSE AppArmor» هي تقديم آخر إلى AppArmor.
- مكان رائع للسؤال حول المساعدة في AppArmor، والاندماج مع مجتمع خواديم أوبنتو هو قناة #ubuntu-server على خادوم Freenode (شبكة IRC).

٥. الشهادات

واحدة من أكثر الأشكال الشائعة للتشفير في وقتنا الراهن هي التشفير وفق المفتاح العمومي (public-key cryptography)؛ يستخدم التشفير وفق المفتاح العمومي مفتاحًا عامًا (public key) ومفتاحًا خاصًا (private key)؛ يعمل النظام بتشفير (encrypt) المعلومات باستخدام مفتاح عمومي، ولا يمكن أن يُفَكّ تشفيرها (decrypted) إلا باستخدام المفتاح الخاص.

استخدام شائع للتشفير وفق المفتاح العمومي هو تشفير البيانات المنقولة باستخدام اتصال SSL (Secure Socket Layer) أو TLS (Transport Layer Security)؛ على سبيل المثال، إن ضبط أباتشي لتوفير HTTPS -بروتوكول HTTP عبر SSL- يسمح بتشفير البيانات في بروتوكول لا يوفر بحد ذاته آليةً للتشفير.

الشهادة (Certificate) هي طريقة تستخدم لتوزيع المفتاح العمومي وغيره من المعلومات عن الخادوم والمنظمة المسؤولة عنه؛ تُوقَّع الشهادات إلكترونيًا بواسطة «سلطة الشهادات» (CA)، إن سلطة الشهادات هي طرفٌ ثالثٌ موثوق تأكد من دقة المعلومات الموجودة في الشهادة.

ا. أنواع الشهادات

لضبط خادوم آمن باستخدام تشفير وفق المفتاح العمومي، عليك إرسال -في أغلب الحالات- طلب الشهادة (متضمنًا المفتاح العمومي الخاص بك) ودليلًا على هوية شركتك ودفعةً ماليةً إلى سلطة شهادات؛ ثم ستتحقق سلطة الشهادات من طلب الشهادة ومن هويتك، ثم ستُرسِل الشهادة إلى خادومك الآمن. بشكلٍ بديل، تستطيع إنشاء شهادتك الموقعة ذاتيًا.

ملاحظة: لاحظ أنه لا يجدر بك استخدام الشهادات الموقعة ذاتيًا في أغلبية بيئات العمل الإنتاجية.

بإكمال مثال HTTPS، ستوفر شهادة موقعة من سلطة الشهادات إمكانيتَين مهمتين لا تملكهما الشهادات الموقعة ذاتيًا:

- المتصفحات تتعرف (عادةً) تلقائيًا على الشهادة وتسمح بإنشاء اتصال آمن دون طلب موافقة المستخدم.
- عندما تعطي سلطة الشهادات شهادةً موقعة، فإنها تضمن هوية المنظمة التي توفر صفحات الويب إلى المتصفح.

أغلبية متصفحات الويب والحواسيب التي تدعم SSL لديها قائمة بسلطات الشهادات التي تُقبَل شهاداتها تلقائيًا؛ إذا واجه المتصفح شهادةً لم تكن سلطة الشهادات التي أصدرتها في قائمته، فإنه (أي المتصفح) سيطلب من المستخدم قبول أو رفض الاتصال؛ وقد تُولِّد بعض التطبيقات الأخرى رسالة خطأ عند استخدام شهادة موقعة ذاتيًا.

عملية الحصول على شهادة من سلطة الشهادات هي عملية سهلة جدًا، لمحة سريعة كالتالي:

١. أنشِئ زوج مفاتيح خاص وعام.
٢. أنشِئ طلب شهادة بناءً على المفتاح العمومي، يحتوي طلب الشهادة على معلومات عن خادومك والشركة التي تستضيفه.
٣. أرسل طلب الشهادة مع الوثائق التي تثبت هويتك إلى سلطة الشهادات؛ لا نستطيع إخبارك أيّة سلطة شهادات عليك أن تختارها؛ ربما يكون قرارك مبنيًا على تجارب سابقة، أو على تجارب أحد أصدقائك أو زملائك، أو على عوامل اقتصادية.

٤. بعـد أن تختـار سـلطة الشـهادات، فعليـك اتبـاع تعليمـاتهم الـتي يوفرونهـا عـن كيفيـة الحصول على شهادة منهم.

٥. بعد أن تتأكد سلطة الشهادات أنك من تدعيّ أنك هو؛ فسيرسلون لك شهادةً رقميةً.

٦. ثبِّت هذه الشهادة على خادومك الآمن، واضبط البرامج الملائمة لاستخدام هذه الشهادة.

ب. توليد طلب توقيع الشهادة (CSR)

إذا كنت ستحصل على شهادة من سلطة شهادات أو كنت ستُوقِّع شهادتك ذاتيًا، فإن أول خطوة هي توليد مفتاح.

إذا كـانت الشـهادة ستُسـتخدَم مـن عفـاريت الخـدمات، مثـل أباتشـي، أو Postfix، أو Dovecot ...إلخ. فإن مفتاحًا بدون عبارة مرور (passphrase) كافٍ عـادةً؛ عدم وجود عبارة مرور تسمح للخدمات أن تبدأ دون تدخل يدوي، وهذه هي الطريقة المفضلة لبدء تشغيل عفريت.

سيغطي هذا القسم طريقة توليد مفتاح مع عبارة مرور، وواحد آخر بدون عبارة مرور؛ ثم سنستخدم المفتاح بدون عبارة مرور لتوليد شهادة ستُستخدَم في مختلف عفاريت الخدمات.

تحذير: تشغيل خدمة آمنة بدون عبارة مرور هو أمر ملائم لأنك لن تحتاج إلى إدخال عبارة المرور كل مرة تبدأ فيها خدمتك الآمنة، لكن هذا غير آمن وأي كشف عن المفتاح سيؤدي إلى جعل الخادوم عرضةً للهجمات.

لتوليد «مفاتيح» لطلب توقيع الشهادة، عليك تنفيذ الأمر الآتي من مِحَث الطرفية:

```
openssl genrsa -des3 -out server.key 2048
Generating RSA private key, 2048 bit long modulus
..........................++++++
.......++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
```

تستطيع الآن إدخال عبارة مرورك، لأفضل قدر من الحماية، يجب أن تحتوي على الأقل على ثمانية محارف؛ الطول الأدنى عند تحديد الخيار des3- هو أربعة محارف؛ ويجب أن تحتوي على أرقام أو على علامات ترقيم ولا تحتوي على كلمة من القاموس؛ تذكر أن عبارة المرور حساسة لحالة الأحرف.

أعد كتابة عبارة المرور للتحقق؛ وبعد إعادة كتابتها بشكل صحيح، فسيُولَّد مفتاح الخادوم وسيُخزَّن في ملف server.key.

أنشِئ الآن مفتاحًا غير آمن (insecure أي بدون عبارة مرور) ثم بدِّل بين أسماء المفاتيح:

```
openssl rsa -in server.key -out server.key.insecure
mv server.key server.key.secure
mv server.key.insecure server.key
```

أصبح الآن اسم ملف المفتاح غير الآمن هو server.key، وسنستخدم هذا الملف لتوليد CSR بدون عبارة مرور.

نفِّذ الأمر الآتي في مِحَث الطرفية لإنشاء CSR:

```
openssl req -new -key server.key -out server.csr
```

ستُسأل عن إدخال عبارة المرور، إذا أدخلت عبارةً صحيحةً، فستُسأل عن إدخال اسم الشركة، واسم الموقع، ومعرف البريد الإلكتروني ...إلخ. بعد أن تُدخِل كل هذه التفاصيل، فسيُنشَأ طلب توقيع الشهادة (CSR) وسيُخزَّن في ملف server.csr.

يجب الآن إرسال ملف طلب توقيع الشهادة إلى سلطة الشهادات لمعالجته؛ ستستخدم سلطة الشهادات ملف طلب توقيع الشهادة لإصدار الشهادة؛ وعلى الكفة الأخرى، تستطيع توليد شهادتك الموقعة ذاتيًا باستخدام طلب توقيع الشهادة السابق.

ج. إنشاء شهادة موقعة ذاتيًا

نفِّذ الأمر الآتي في الطرفية لإنشاء شهادة موقعة ذاتيًا:

```
openssl x509 -req -days 365 -in server.csr -signkey server.key \
-out server.crt
```

سيسألك الأمر السابق عن عبارة المرور، بعد أن تدخل عبارة المرور الصحيحة، فستُنشَأ الشهادة وتُخزَّن في ملف server.crt.

تحذير: إذا استُخدِم خادومك الآمن في بيئة إنتاجية، فربما تحتاج إلى شهادة موقع من سلطة الشهادات (CA)، ليس من المستحسن استخدام شهادة موقعة ذاتيًا.

د. تثبيت الشهادة

تستطيع تثبيت ملف المفتاح server.key وملف الشهادة server.crt أو ملف الشهادة المُصدَر من سلطة الشهادات، بتنفيذ الأمرين الآتيين في الطرفية:

```
sudo cp server.crt /etc/ssl/certs
sudo cp server.key /etc/ssl/private
```

اضبط الآن ببساطة أيّة تطبيقات فيها إمكانية استخدام التشفير وفق المفتاح العمومي لكي تستخدم ملفات الشهادة والمفتاح؛ على سبيل المثال، يمكن أن يزود أباتشي HTTPS، و Dovecot يستطيع أن يزود IMAPS و POP3S ...إلخ.

ه. سلطة الشهادات

إذا كانت تتطلب الخدمات على شبكتك أكثر من مجرد بضع شهادات موقعة ذاتيًا، فربما يكون من المفيد بذل جهد إضافي وإعداد سلطة شهادات داخلية؛ ستسمح الشهادات الموقعة من سلطة الشهادات الخاصة بك لمختلف الخدمات باستخدام الشهادات لكي تثق بسهولة بالخدمات الأخرى التي تملك شهادات مُصدَرة من نفس سلطة الشهادات.

أنشِئ أولًا المجلدات التي سنضع فيها شهادة سلطة الشهادات والملفات المتعلقة بذلك:

```
sudo mkdir /etc/ssl/CA
sudo mkdir /etc/ssl/newcerts
```

تحتاج سلطة الشهادات إلى بضعة ملفات إضافية لكي تعمل، واحدٌ لكي يتعقب آخر رقم تسلسلي أُستخدِم من سلطة الشهادات، إذ يجب أن تملك كل شهادة رقمًا تسلسليًا فريدًا؛ وملفٌ آخر لتسجيل الشهادات التي أُصدِرَت:

```
sudo sh -c "echo '01' > /etc/ssl/CA/serial"
sudo touch /etc/ssl/CA/index.txt
```

الملف الثالث هو ملف ضبط سلطة الشهادات، على الرغم من أنه ليس مطلوبًا، لكن من المنطقي وجوده عند إنشاء عدّة شهادات؛ عدِّل ملف /etc/ssl/openssl.cnf وفي قسم [CA_default]، غيِّر ما يلي:

```
dir          = /etc/ssl/              # Where everything is kept
database     = $dir/CA/index.txt      # database index file.
certificate = $dir/certs/cacert.pem # The CA certificate
serial       = $dir/CA/serial         # The current serial number
private_key = $dir/private/cakey.pem # The private key
```

ثم أنشِئ الشهادة الجذر الموقعة ذاتيًا:

```
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem \
-out cacert.pem -days 3650
```

ستُسأل عن إدخال التفاصيل حول الشهادة.

الآن ثبت الشهادة الجذر والمفتاح:

```
sudo mv cakey.pem /etc/ssl/private/
```

```
sudo mv cacert.pem /etc/ssl/certs/
```

أنت الآن جاهزٌ لبدء توقيع الشهادات، أول شيء مطلوب هو «طلب توقيع الشهادة» (راجع القسم السابق لمزيد من المعلومات)، بعد أن تحصل على طلب توقيع الشهادة، فأدخِل ما يلي لتوليد شهادة موقعة من سلطة الشهادات:

```
sudo openssl ca -in server.csr -config /etc/ssl/openssl.cnf
```

بعد إدخال كلمة المرور لمفتاح سلطة الشهادات، فستُسأل عن توقيع الشهادة، ومرةً أخرى لإصدار الشهادة، يجب أن ترى كميةً كبيرةً من المخرجات المتعلقة بإنشاء الشهادة.

يجب أن يكون هنالك ملف جديد هو /etc/ssl/netcerts/01.pem يحتوي على نفس المخرجات، انسخ والصق كل شيء من بداية السطر -----BEGIN CERTIFICATE----- إلى السطر -----END CERTIFICATE----- إلى ملف مسمى بنفس اسم المضيف لخادومك مكان تثبيت الشهادة؛ فمثلًا الاسم mail.example.com.crt هو اسم وصفي جيد.

الشهادات المتتالية ستُسمى 02.pem، و 03.pem ...إلخ.

ملاحظة: استبدل mail.example.com.crt بالاسم الوصفي الخاص بك.

في النهاية، انسخ الشهادة الجديدة إلى المضيف الذي يحتاج لها واضبط الخدمات الملائمة لكي تستخدمها، المكان الافتراضي لتثبيت الشهادات هو /etc/ssl/certs، وهذا ما سيُمكِّن عدّة خدمات من استخدام نفس الشهادة دون تعقيد أذونات الملف.

للتطبيقات التي يمكن ضبطها لاستخدام شهادة CA، يجب أن تَنسخ أيضًا الملف التالي

/etc/ssl/certs/cacert.pem إلى مجلد /etc/ssl/certs/ على كل خادوم.

و. مصادر

- لتعليمات تفصيلية عن استخدام التشفير، راجع صفحة «SSL Certificates HOWTO».
- صفحة ويكيبيديا HTTPS لديها المزيد من المعلومات حول HTTPS.
- للمزيد من المعلومات حول OpenSSL، راجع الصفحة الرئيسية لموقع OpenSSL.
- كتاب «Network Security with OpenSSL» من O'Reilly هو مرجع معمّق.

٦. نظام ملفات eCryptfs

إن eCryptfs هو نظام ملفات للتشفير متوافق مع معايير POSIX ومن فئة الشركات لنظام لينُكس؛ وبتشكيل طبقة فوق طبقة نظام الملفات، فإن eCryptfs يحمي الملفات بغض النظر عن نظام الملفات المُستخدَم أو نوع القسم ...إلخ.

هنالك خيار أثناء التثبيت لتشفير قسم home/، هذا سيضبط تلقائيًا كل شيء يحتاج له النظام لتشفير ووصل ذاك القسم. سنشرح هنا طريقة الضبط لتشفير srv/ باستخدام eCryptfs.

أ. استخدام eCryptfs

أولًا، ثبّت الحزم اللازمة، بإدخال الأمر الآتي من الطرفية:

```
sudo apt-get install ecryptfs-utils
```

الآن صِل القسم الذي تريد تشفيره:

```
sudo mount -t ecryptfs /srv /srv
```

ستُسأل الآن عن بعض التفاصيل حول كيفية تشفير البيانات.

لاختبار أن الملفات الموجودة في srv/ هي مشفرة، فانسخ المجلد etc/default/ إلى srv/:

```
sudo cp -r /etc/default /srv
```

ثم افصل القسم /srv، وحاول عرض الملف:

```
sudo umount /srv
cat /srv/default/cron
```

إعادة وصل /srv باستخدام ecryptfs ستجعل البيانات قابلةً للعرض مرةً أخرى.

ب. وصل الأقسام المشفرة تلقائيًا

هنالك طريقتان لوصل نظام ملفات مُشفَّر باستخدام ecryptfs أثناء الإقلاع؛ سيستخدم هذا المثال الملف /root/.ecryptfsrc الذي يحتوي على خيارات الوصل، بالإضافة إلى ملف مرور موجود على قرص USB.

أنشِئ أولًا الملف /root/.ecryptfsrc الذي يحتوي على:

```
key=passphrase:passphrase_passwd_file=/mnt/usb/passwd_file.txt
ecryptfs_sig=5826dd62cf81c615
ecryptfs_cipher=aes
ecryptfs_key_bytes=16
ecryptfs_passthrough=n
ecryptfs_enable_filename_crypto=n
```

ملاحظة: عدِّل ecryptfs_sig إلى التوقيع في /root/.ecryptfs/sig-cache.txt.

ثم أنشِئ ملف المرور /mnt/usb/passwd_file.txt:

```
passphrase_passwd=[secrets]
```

أضف الآن الأسطر الضرورية إلى ملف /etc/fstab:

```
/dev/sdb1  /mnt/usb    ext3       ro         0 0
/srv       /srv        ecryptfs   defaults   0 0
```

تأكد أن قرص USB سيوصل قبل القسم المشفر.

في النهاية، أعد الإقلاع ويجب أن يوصل /srv باستخدام eCryptfs.

ج. أدواتٌ أخرى

الحزمة ecryptfs-utils تحتوي على أدواتٍ أخرى مفيدة:

- الأداة ecryptfs-setup-private تُنشِئ مجلد ~/Private الذي يحتوي على المعلومات المشفرة؛ يمكن تنفيذ هذه الأداة من المستخدمين العاديين للحفاظ على بياناتهم من المستخدمين الآخرين على النظام.
- الأداة ecryptfs-mount-private و ecryptfs-umount-private ستصل أو تفصل مجلد ~/Private على التوالي وبالترتيب.
- ecryptfs-add-passphrase: إضافة عبارة مرور لما يسمى «kernel keyring».
- ecryptfs-manager: إدارة كائنات eCryptfs مثل المفاتيح.
- ecryptfs-stat: السماح لك بعرض معلومات eCryptfs الوصفية لملفٍ ما.

د. مصادر

- للمزيد من المعلومات حول eCryptfs، راجع صفحة المشروع على Lanuchpad.
- هنالك مقالة في Linux Journal تشرح eCryptfs.
- للمزيد من خيارات eCryptfs، راجع صفحة الدليل man ecryptfs.
- لدى صفحة ويكي أوبنتو «eCryptfs» المزيد من التفاصيل.

١٠

المراقبة

المراقبة هي جزء مهم من إدارة الخواديم والخدمات الأساسية؛ تُراقَب معظم الخدمات الشبكية للأداء (performance) أو التوفر (availability) أو كليهما؛ سيَشرح هذا الفصل طريقة تثبيت وضبط Nagios لمراقبة التوفر، و Munin لمراقبة الأداء.

سنستخدم في أمثلة هذا الفصل خادومين بأسماء server01 و server02؛ سيُضبَط server01 مع Nagios لمراقبة الخدمات التي عليه وعلى الخادوم server02؛ وسيُضبَط server01 مع Munin لجمع المعلومات من الشبكة، باستخدام حزمة munin-node، وسيُضبَط server02 لكي يُرسِل المعلومات إلى server01.

نأمل أن تساعدك هذه الأمثلة البسيطة في مراقبة الخواديم والخدمات الإضافية في شبكتك.

ا. ناجيوس Nagios

ا. التثبيت

أولًا، ثبت الحزمة nagios على خادوم server01، وذلك بإدخال الأمر الآتي في الطرفية:

```
sudo apt-get install nagios3 nagios-nrpe-plugin
```

سيُطلَب منك إدخال كلمة مرور لمستخدم nagiosadmin، تصاريح المستخدم مخزنة في /etc/nagios3/htpasswd.users. ولتعـــديل كلمـــة مـــرور nagiosadmin أو إضـــافة مستخدمين آخرين إلى سكربتات Nagios CGI، فاستخدم htpasswd الذي هو جزء من حزمة apache2-utils.

على سبيل المثال، لتغيير كلمة المرور لمستخدم nagiosadmin:

```
sudo htpasswd /etc/nagios3/htpasswd.users nagiosadmin
```

لإضافة مستخدم جديد:

```
sudo htpasswd /etc/nagios3/htpasswd.users steve
```

الآن على خادوم server02، ثبّت الحزمة nagios-nrpe-server؛ بتنفيذ الأمر الآتي على server02:

```
sudo apt-get install nagios-nrpe-server
```

ملاحظة: سيسمح NRPE لك بتنفيذ فحوصات محلية على الأجهزة البعيدة، هنالك طرق أخرى للقيام بذلك عبر إضافات Nagios أخرى.

ب. لمحة عن الضبط

هنالك عدة مجلدات تحتوي على ضبط Nagios وملفات التحقق (check files).

- /etc/nagios3: يحتوي على ملفات الضبط لعمل عفريت nagios، وملفات CGI، والمضيفين ...إلخ.
- /etc/nagios-plugins: يحتوي ملفات الضبط للتحقق من الخدمات.
- /etc/nagios: في المضيفين البعيدين، ويحتوي على ملفات ضبط nagios-nrpe-server.
- /usr/lib/nagios/plugins/: المكان الذي تخزَّن فيه ملفات التحقق الثنائية، استخدم الخيار h- لمشاهدة المساعدة لتحققٍ ما.

مثال:

```
/usr/lib/nagios/plugins/check_dhcp -h
```

هنالك وفرة في التحققات التي يمكن ضبط Nagios ليجريها على أي مضيف؛ سيُضبَط Nagios في هذا المثال للتحقق من مساحة القرص الصلب المتوفرة و DNS و MySQL؛ سيُجرى تحقق DNS على server02 وتحقق MySQL على server01 و server02.

ملاحظة: راجع «الفصل الحادي عشر: خواديم الويب» لمزيدٍ من المعلومات حول ضبط خادوم أباتشي، وراجع «الفصل الثامن» لمعلومات حول DNS، والفصل الثاني عشر لمعلومات حول MySQL.

هنالك بعض المصطلحات التي عندما تُشرَح ستُسهِّل فهم ضبط Nagios:

- المضيف (host): خادوم أو محطة عمل (workstation)، أو جهاز شبكي ...إلخ. الذي يُراقَب.
- مجموعة مضيفين (host group): مجموعة من المضيفين المتشابهين؛ على سبيل المثال، تستطيع أن تُجمِّع كل خواديم الويب أو خواديم الملفات ...إلخ.
- الخدمة (service): الخدمة التي تُراقَب في المضيف، مثل HTTP أو DNS أو NFS ...إلخ.
- مجموعة الخدمات (service group): تسمح لك بجمع عدّة خدمات متشابهة مع بعضها بعضًا، هذا مفيد لتجميع عدّة خدمات HTTP على سبيل المثال.
- جهة الاتصال (contact): الشخص الذي سيُنبَّه عندما يحدث حدثٌ ما؛ يمكن ضبط Nagios ليرسل بريدًا إلكترونيًا أو رسائل SMS ...إلخ.

افتراضيًا، يكون ضبط Nagios ليتحقق من HTTP، والمساحة التخزينية المتوفرة في القرص، و SSH، والمستخدمين الحاليين، والعمليات، والحِمل على localhost؛ سيتحقق Nagios أيضًا من البوابة بعمل ping لها.

تثبيتات Nagios الضخمة قد يصبح ضبطها معقدًا جدًا، لذلك من الأفضل عادةً البدء بمضيف واحد أو اثنين ثم التوسع بعد ضبطهما جيدًا.

ج. الضبط

١. أولًا، أنشئ ملف ضبط للمضيف للخادوم server02؛ ما لم يُذكر عكس ذلك، فعليك تنفيذ هذه الأوامر على server01؛ أدخِل ما يلي في الطرفية:

```
sudo cp /etc/nagios3/conf.d/localhost_nagios2.cfg \
/etc/nagios3/conf.d/server02.cfg
```

ملاحظة: في الأوامر السابقة أو التالية استبدل «server01» و «server02» و 172.18.100.100 و 172.18.100.101 بأسماء المضيفين وعناوين IP لخادومَيك.

ثم عدِّل الملف /etc/nagios3/conf.d/server02.cfg:

```
define host {
    use            generic-host     ; Name of host template to
use
    host_name      server02
    alias          Server 02
    address        172.18.100.101
}
    # check DNS service.
    define service {
        use                          generic-service
        host_name                    server02
        service_description          DNS
        check_command                check_dns!172.18.100.101
    }
```

أعد تشغيل عفريت nagios لتفعيل الضبط الجديد:

```
sudo service nagios3 restart
```

أضف الآن تعريفًا للتحقق من MySQL بإضافة ما يلي إلى /etc/nagios3/conf.d/

services_nagios.cfg:

```
# check MySQL servers.
define service {
    hostgroup_name         mysql-servers
    service_description    MySQL
    check_command          check_mysql_cmdlinecred!nagios!
secret!$HOSTADDRESS
    use                    generic-service
    notification_interval 0 ; set > 0 if you want to be
renotified
}
```

يجب الآن تعريف مجموعة المضيفين mysql-servers؛ عدِّل الملف /etc/nagios3/conf.d/ hostgroups_nagios2.cfg مضيفًا:

```
# MySQL hostgroup.
define hostgroup {
     hostgroup_name     mysql-servers
     alias              MySQL servers
     members            localhost, server02
}
```

٣. يحتاج Nagios لأن يستوثق إلى MySQL، فأضف مستخدم nagios إلى MySQL بإدخال الأمر:

```
mysql -u root -p \
-e "create user nagios identified by 'secret';"
```

ملاحظة: يجب أن يتواجد المستخدم nagios في كل المضيفين في مجموعة mysql-servers.

أعد تشغيل nagios ليبدأ التحقق من خواديم MySQL:

```
sudo service nagios3 restart
```

أخيرًا، اضبط NRPE للتحقق من المساحة الفارغة في القرص على الخادوم server02.

أضف التحقق من الخدمة في server01 في ملف /etc/nagios3/conf.d/server02.cfg:

```
# NRPE disk check.
define service {
    use                     generic-service
    host_name               server02
    service_description     nrpe-disk
    check_command           check_nrpe_1arg!check_all_disks!
172.18.100.101
}
```

الآن على الخادوم server02، عدِّل الملف /etc/nagios/nrpe.cfg مغيّرًا:

```
allowed_hosts=172.18.100.100
```

ثم في منطقة تعريف الأمر أضف ما يلي:

```
command[check_all_disks]=/usr/lib/nagios/plugins/check_disk -w
20% -c 10% -e
```

في النهاية، أعد تشغيل nagios-nrpe-server:

```
sudo service nagios-nrpe-server restart
```

وأيضًا على الخادوم server01 أعد تشغيل nagios:

```
sudo service nagios3 restart
```

يجب أن تكون قادرًا على رؤية المضيف والتحقق من الخدمات في ملفات Nagios CGI؛ للوصول إليهم، وجِّه متصفحك إلى http://server01/nagios3؛ ثم ستُسأل عن اسم مستخدم nagiosadmin وكلمة مروره.

د. مصادر

- لم يشرح هذا القسم إلا القليل من ميزات Nagios؛ تحتوي الحزمتين nagios-plugins-extra و nagios-snmp-plugins على المزيد من تحققات الخدمات.
- للمزيد من المعلومات، راجع موقع Nagios، تحديدًا موقع «التوثيق».
- هنالك قائمة بالكتب المتعلقة بمراقبة الشبكة و Nagios.
- صفحة ويكي أوبنتو «Nagios» فيها بعض التفاصيل الإضافية.

٢. مونين Munin

ا. التثبيت

قبل تثبيت Munin على server01، فيجب أن يُثبَّت قبله apache2؛ الضبط الافتراضي كافٍ لتشغيل خادوم munin.

أولًا، ثبت munin على الخادوم server01 بإدخال الأمر:

```
sudo apt-get install munin
```

الآن ثبِّت الحزمة munin-node على الخادوم server02:

```
sudo apt-get install munin-node
```

ب. الضبط

عدِّل الملف /etc/munin/munin.conf على الخادوم server01 مُضيفًا عنوان IP للخادوم server02:

```
## First our "normal" host.
[server02]
    address 172.18.100.101
```

ملاحظة: استبدل server02 و 172.18.100.101 باسم المضيف وعنوان IP الحقيقي لخادومك.

الآن اضبط munin-node على الخادوم server02، بتعديل /etc/munin/munin-node.conf للسماح بالوصول إلى الخادوم server01:

```
allow ^172\.18\.100\.100$
```

ملاحظة: استبدل $^172\.18\.100\.100$ بعنوان IP لخادوم Munin الخاص بك.

أعد تشغيل munin-node على server02 لكي تأخذ التعديلات مجراها:

```
sudo service munin-node restart
```

في النهاية، وجِّه متصفحك إلى http://server01/munin، يجب أن ترى روابط إلى مخططات بيانية جميلة تعرض معلومات من الحزمة القياسية munin-plugins للقرص والشبكة والعمليات والنظام.

ملاحظة: لما كان هذا التثبيت حديثًا، فربما ستحتاج لبعض الوقت لعرض معلومات مفيدة.

ج. إضافات أخرى

تحتوي حزمة munin-plugins-extra على تحققات من أداء خدماتٍ إضافية مثل DNS، و DHCP، وسامبا ...إلخ. أدخل الأمر الآتي لتثبيت هذه الحزمة:

```
sudo apt-get install munin-plugins-extra
```

تأكد من تثبيت هذه الحزمة على جهازَيّ الخادوم والعقدة.

د. مصادر

- راجع موقع Munin لمزيدٍ من التفاصيل.
- تحديدًا صفحة «توثيق Munin» التي تحتوي على معلومات عن الإضافات الأخرى، وكيفية كتابة إضافات ... إلخ.
- مصدر آخر هو صفحة ويكي أوبنتو «Munin».

11

خواديم الويب

خـادوم الـويب هـو برمجيـة مسـؤولة عـن قبـول طلبـات HTTP مـن العملاء المعروفيـن بمتصفحات الويب، وتخديمهم بردود HTTP مع محتويات البيانات الاختيارية؛ التي تكون عـادةً صفحات ويب كمستندات HTML والكائنات الأخرى مثل الصور والفيديو ...إلخ.

١. خادوم أباتشي HTTPD

أباتشي (Apache) هو أشهر خـادوم ويب مستخدم في أنظمة لينُكس؛ تُستعمَل خـواديم الـويب لتخـديم الصـفحات المطلوبـة مـن العملاء؛ يَطلـب ويَعـرض العملاءُ صـفحاتَ الـويب عـادةً باستخدام متصفح ويب مثل فايرفكس أو كروميوم أو أوبرا أو موزيلا.

يُـدخِل المستخدم URL (اختصـار للعبـارة Uniform Resource Locator) للإشـارة إلـى خـادوم ويـب باسم النطـاق الكامـل (FQDN) والمسـار إلـى الهـدف المطلـوب؛ علـى سـبيل المثـال، لعرض الصفحة الرئيسية لموقع أوبنتو، فسيدخل المستخدم اسم النطاق الكامل فقط:

```
www.ubuntu.com
```

لعرض الصفحة الفرعية للمجتمع، فإن المستخدم سيُدخِل اسم النطاق الكامل متبوعًا بمسار:

```
www.ubuntu.com/community
```

أشهر بروتوكول مُستخدَم لنقل صفحات الويب هو بروتوكول نقل النص الفائق (Hyper Text Transfer Protocol، اختصارًا HTTP)، بروتوكولات أخرى مدعومة مثل بروتوكول نقل النص الفائق فوق طبقة مقابس آمنة (Hyper Text Transfer Protocol over Secure Sockets Layer، اختصارًا HTTPS)، وبروتوكول نقل الملفات (File Transfer Protocol، اختصارًا FTP) الذي هو بروتوكول لرفع (upload) أو تنزيل (download) الملفات.

يُستخدَم خادوم ويب أباتشي عادةً مع محرك قواعد بيانات MySQL، ولغة معالجة النصوص الفائقة (PHP)، وغيرها من «لغات السكربتات» (scripting languages) مثل بايثون و بيرل؛ يُسمَّى هذا الضبط بالمصطلح LAMP (Linux, Apache, MySQL and Perl/Python/PHP) ويُشكِّل منصةً قوية ومرنةً لتطوير ونشر تطبيقات الويب.

التثبيت

خادوم أباتشي متوفر في أوبنتو؛ أدخل الأمر الآتي لتثبيته:

```
sudo apt-get install apache2
```

الضبط

يُضبَط أباتشي بوضع تعليمات (directives) في ملفات ضبط نصية بسيطة؛ هذه التعليمات موزعة بين الملفات والمجلدات الآتية:

- ملف apache2.conf: ملف ضبط أباتشي الرئيسي؛ يحتوي على الإعدادات العامة لأباتشي.
- الملف httpd.conf: تاريخيًا كان ملف ضبط أباتشي الرئيسي؛ وسُمِّي هذا الملف باسم عفريت httpd؛ الآن الملفُ فارغٌ افتراضيًا، حيث نُقِلَت معظم خيارات الضبط إلى المجلدات تالية الذكر؛ يمكن أن يُستخدَم هذا الملف لإعدادات الضبط التي يجريها المستخدم وتؤثر على ضبط أباتشي العام.

- المجلد conf-available: يحتوي على ملفات الضبط المتوفرة لأباتشي؛ جميع الملفات التي كانت في مجلد /etc/apache2/conf.d انتقلت إلى /etc/apache2/conf-available.

- المجلد conf-enabled: يحتوي على الوصلات الرمزية للملفات في مجلد /etc/apache2/conf-available/؛ فعندما تُضاف وصلة رمزية لملف ضبط، فإنه سيُفعَّل عندما يُعاد تشغيل خدمة أباتشي.

- الملف envvars: الملف حيث تُضبَط قيم متغيرات البيئة (environment variables) لأباتشي.

- مجلد mods-available: يحتوي هذا المجلد على ملفات خاصة لتحميل الوحدات (modules) وضبطها، لا تملك جميع الوحدات ملفات ضبط خاصة بها.

- مجلد mods-enabled: يحتوي على الوصلات الرمزية إلى الملفات في /etc/apache2/mods-available/؛ فعندما تُضاف وصلة رمزية لملف ضبط خاص بوحدة، فإن هذه الوحدة ستُفعَّل في المرة القادمة التي سيُعاد تشغيل أباتشي فيها.

- ملف ports.conf: يحتوي على التعليمات التي تُحدِّد منافذ TCP التي يستمع إليها أباتشي.

- مجلد sites-available: يحتوي هذا المجلد على ملفات الضبط «للمضيفين الوهميين» (Virtual Hosts) في أباتشي؛ يسمح المضيفون الوهميون بضبط أباتشي لتشغيل عدة مواقع تملك ضبطًا منفصلًا.

- مجلد sites-enabled: مثل mods-enabled، يحتوي مجلد sites-enabled على وصلاتٍ رمزية لمحتويات مجلد /etc/apache2/sites-available؛ وبشكل مشابه، فإن ملفات الضبط التي تُوصَل وصلًا رمزيًا لهذا المجلد ستُفعَّل في المرة القادمة التي سيُعاد تشغيل خادوم أباتشي فيها.

- الملف magic: يُستخدَم لتحديد نوع MIME بناءً على أول عدّة بايتات من الملف.

بالإضافة لذلك، يمكن أن تُضاف ملفات ضبط أخرى باستخدام التعليمة Include؛ ويمكن أن تُستخدم المحارف الخاصة (wildcards) لتضمين العديد من ملفات الضبط؛ أي تعليمة يمكن أن توضع في أيّ من ملفات الضبط تلك. لا تؤخذ التعديلات على ملفات الضبط الرئيسية بعين الاعتبار من أباتشي إلا إذا بدء أو أعيد تشغيله.

يقرأ الخادوم أيضًا ملفًا يحتوي على أنواع المستندات (mime types)؛ يُحدَّد اسم الملف بالتعليمة TypesConfig ويكون عمومًا هو الملف /etc/apache2/mods-available/mime.conf؛ الذي ربما يحتوي على إضافات أو تعديلات على /etc/mime.types.

الإعدادات الأساسية

يشرح هذا القسم معاملات ضبط خادوم أباتشي الأساسية؛ ارجع إلى توثيق أباتشي للمزيد من التفاصيل.

يأتي أباتشي مع ضبط افتراضي «صديق» للمضيفين الوهميين؛ هذا يعني أنه مضبوط مع مضيف وهمي وحيد افتراضيًا (باستخدام التعليمة VirtualHost) الذي يمكن أن يعدَّل أو يُستخدَم كما هو لو أردت الحصول على موقع وحيد فقط؛ أو تستطيع استخدامه كقالب للمضيفين الوهميين الإضافيين إذا كنت تريد الحصول على عدّة مواقع؛ إذا تُرِكَ كما هو، فسيُخدِّم المضيف الوهمي الافتراضي موقعك الافتراضي؛ أو الموقع الذي سيراه مستخدمو الموقع لو أن عنوان URL الذي أدخلوه لا يُطابِق التعليمة ServerName لأيٍّ من مواقعك المخصصة؛ لتعديل المضيف الوهمي الافتراضي فيجب تعديل الملف /etc/apache2/sites-available/default.

ملاحظة: التعليمات المضبوطة لمضيفٍ وهمي لا تطبَّق إلا عليه فقط؛ إذا ضُبِطَت تعليمة لعموم الخادوم ولم يعاد تعريفها في ضبط المضيف الوهمي، فسيُستخدَم الضبط الافتراضي؛ على سبيل المثال، تستطيع ضبط عنوان بريد webmaster ولا تُعيد تعريفه لكل مضيف وهمي.

إذا أردت ضبط مضيفٍ وهميٍ جديد أو موقع؛ فانسخ هذا الملف إلى نفس المجلد باسمٍ من اختيارك؛ على سبيل المثال:

```
sudo cp /etc/apache2/sites-available/000-default.conf \
/etc/apache2/sites-available/mynewsite.conf
```

عدِّل ملف ضبط الموقع الجديد باستخدام بعض التعليمات المشروحة في الأسفل.

التعليمة ServerAdmin تحدد البريد الإلكتروني لمدير الخادوم؛ القيمة الافتراضية هي webmaster@localhost؛ يجب أن تُعدَّل القيمة إلى البريد الإلكتروني الخاص بك (إذا كنت مديرًا للنظام)؛ إذا حدثت مشكلة مع موقع الويب، فسيُظهِر أباتشي رسالة خطأ تحتوي على هذا البريد الإلكتروني للتبليغ عن المشكلة؛ اعثر على هذه التعليمة في ملف ضبط الموقع الخاص بك في /etc/apache2/sites-available.

التعليمة listen تحدد المنفذ وبشكل اختياري عنوان IP الذي يجب على أباتشي الاستماع إليه؛ إذا لم يُحدَّد عنوان IP، فسيستمع أباتشي على جميع عناوين IP المُسندَة للخادوم الذي يعمل عليه أباتشي؛ القيمة الافتراضية للتعليمة listen هي ٨٠؛ عدِّل هذه القيمة إلى 127.0.0.1:80 لجعل أباتشي يستمع فقط إلى بطاقة loopback لذلك لن يكون متوفرًا إلى الإنترنت، عدِّل القيمة إلى ٨١ (على سبيل المثال) لتغيير المنفذ الذي يستمع إليه أباتشي؛ أو اتركه كما هو للعمل العادي؛ هذه التعليمة توجد وتُعدَّل في ملفها الخاص /etc/apache2/ports.conf.

التعليمة ServerName هي اختيارية وتحدد ما هو اسم النطاق الكامل (FQDN) لموقعك الذي سيستجيب أباتشي له؛ المضيف الوهمي الافتراضي لا يملك خاصية ServerName مُحدَّدة، لذلك سيستجيب لجميع الطلبات التي لا تطابقها التعليمة ServerName في أي مضيف وهمي آخر؛ إذا حصل وامتلكتَ النطاق ذو الاسم ubunturocks.com وأردت أن تستضيف الموقع على خادومك، فإن قيمة ServerName في ملف ضبط المضيف الوهمي الخاص بك ستكون ubunturocks.com، أضف هذه التعليمة إلى ملف ضبط المضيف الوهمي الجديد الذي أنشَأناه سابقًا (/etc/apache2/sites-available/mynewsite.conf).

ربما تريد من موقعك أن يستجيب إلى www.ubunturocks.com، ولما كان العديد من المستخدمين يعتبرون أنّ السابقة www هي سابقة ملائمة لمواقع الويب؛ فعليك استخدام التعليمة ServerAlias لهذا الغرض؛ ربما تستخدم المحارف الخاصة (wildcards) للتعليمة ServerAlias.

فمثلًا، سيسبب الضبط الآتي استجابة موقعك لأي طلب نطاق ينتهي بالعبارة «‎.ubunturocks.com»:

```
ServerAlias *.ubunturocks.com
```

تُحدِّد التعليمة DocumentRoot أين يجب أن يبحث أباتشي عن الملفات لإنشاء الموقع؛ القيمة الافتراضية هي ‎/var/www كما هو محدد في ‎/etc/apache2/sites-available/000-default.conf؛ يمكنك تستطيع تعديل هذه القيمة في ملف ضبط مضيفك الوهمي؛ لكن تذكر أن تُنشِئ المجلد إذا كان ذلك ضروريًا.

فعِّل المضيف الوهمي الجديد باستخدام الأداة a2ensite وأعد تشغيل أباتشي:

```
sudo a2ensite mynewsite
sudo service apache2 restart
```

ملاحظة: تأكد أنك ستستبدل mynewsite باسم أكثر وصفًا للمضيف الوهمي؛ إحدى الطرق لتسمية الملف هي استخدام قيمة ServerName للمضيف الوهمي.

وبشكلٍ مشابه، استخدم الأداة a2dissite لتعطيل المواقع؛ يمكن أن يكون هذا مفيدًا عند استكشاف أخطاء الضبط عند وجود أكثر من مضيف وهمي:

```
sudo a2dissite mynewsite
sudo service apache2 restart
```

الإعدادات الافتراضية

سيشرح هذا القسم إعدادات الضبط الافتراضية لخادوم أباتشي؛ مثلًا، إذا أضفت مضيفًا وهميًا فالإعدادات التي ستضبطها للمضيف الوهمي ستكون لها الأولوية لذاك المضيف الوهمي؛ وستُستخدَم القيمة الافتراضية للتعليمات غير المُعرَّفة ضمن إعدادات المضيف الوهمي.

التعليمة DirectoryIndex هي الصفحة الافتراضية المُخدَّمة من الخادوم عندما يَطلب المستخدم فهرس الدليل بإدخال شرطة أمامية (/) في نهاية اسم الدليل.

على سبيل المثال، عندما يطلب المستخدم الصفحة http://www.example.com/directory/ فأنه إما سيحصل على صفحة DirectoryIndex إن وجدت، أو على قائمة بمحتويات المجلد مولدَّةً من الخادوم إذا لم تكن موجودةً وكان قد حُدِّد الخيار Indexes، أو صفحة «Permission Denied» إن لم يتحقق أيٌّ منهما. سيحاول الخادوم إيجاد أحد الملفات المذكورة في التعليمة DirectoryIndex وستُعيد أول ملف ستجده؛ إذا لم تجد أي ملف من تلك الملفات وكان الخيار «Options Indexes» مضبوطًا لهذا المجلد، فسيولِّد الخادوم قائمةً بصيغة HTML للمجلدات الفرعية والملفات في هذا الدليل؛ القيمة الافتراضية الموجودة في ملف /etc/apache2/mods-available/dir.conf هي "index.html index.cgi index.pl index.php index.xhtml index.htm" وبالتالي إذا عَثَر أباتشي على ملف في المجلد المطلوب يطابق أحد تلك الأسماء، فسيُظهِر أول مطابقة.

التعليمة ErrorDocument تسمح لك بتحديد ملف لكي يستعمله أباتشي عند حدوث خطأ معين؛ على سبيل المثال، إذا طلب المستخدم ملفًا غير موجودٍ، فسيحدث خطأ ٤٠٤؛ وافتراضيًا، سيُعيد أباتشي الرمز HTTP 404؛ راجع /etc/apache2/conf.d/localized-error-pages لمعلومات تفصيليّة عن استخدام ErrorDocument بما فيها أماكن ملفات الأمثلة.

يكتب الخادوم سجل النقل افتراضيًا إلى الملف /var/log/apache2/access.log، تستطيع تغيير هذا لكل موقع بناءً على ملفات ضبط مضيفك الوهمي باستخدام التعليمة CustomLog؛ أو أن تقبل باستخدام القيمة الافتراضية المحددة في /etc/apache2/conf.d/other-vhosts-access-log. ربما تحدد أيضًا الملف الذي تريد تسجيل الأخطاء إليه باستخدام التعليمة ErrorLog، التي تكون قيمتها الافتراضية هي /var/log/apache2/error.log؛ لكن اترك هذا السجل منفصلًا عن سجل النقل للمساعدة في استكشاف الأخطاء الحاصلة مع خادوم أباتشي؛ ربما تحدد أيضًا التعليمة LogLevel (القيمة الافتراضية هي "warn") و LogFormat (راجع /etc/apache2/apache2.conf للقيمة الافتراضية).

تُحدَّد بعض الخيارات على أساس المجلد بدلًا من الخادوم؛ التعليمة Options هي إحداها، يكون قسم Directory محاطًا بوسوم شبيهة بلغة XML، كما يلي:

```
<Directory /var/www/mynewsite>
...
</Directory>
```

التعليمة Options ضمن قسم Directory تقبل قيمة واحدة أو أكثر من القيم الآتية مفصولةً بفراغات:

- ExecCGI السماح بتنفيذ سكربتات CGI، لن تُنفَّذ سكربتات CGI ما لم يُحدَّد هذا الخيار.

تنويه: لا يجب أن تُنفَّذ أغلبية الملفات كسكربتات CGI، لأن ذلك سيكون خطرًا جدًا! سكربتات CGI يجب أن تُبقى في مجلد منفصل وخارج المجلد الجذر لموقعك، ويجب أن يكون الخيار ExecCGI مضبوطًا لهذا المجلد فقط؛ هذا هو الضبط الافتراضي، والمكان الافتراضي لسكربتات CGI هو /usr/lib/cgi-bin/.

- Includes: السماح بتضمينات من جهة الخادوم؛ حيث تسمح تضمينات الخادوم لملف HTML بتضمين الملفات الأخرى، راجع «Apache SSI Documentation» لمزيدٍ من المعلومات.

- IncludesNOEXEC: السماح بتضمينات من جهة الخادوم، لكن تعطيل الأمرَين #exec و #include في سكربتات CGI.

- Indexes: عرض قائمة مُنسَّقة بمحتويات المجلد، إذا لم يُعثر على ملف DirectoryIndex (مثل index.html) في المجلد المطلوب.

تحذير: لأغراض تتعلق بالحماية، لا يجب أن يُضبَط هذا الخيار عادةً؛ وخصوصًا في مجلد جذر الموقع! فعِّل هذا الخيار بحذر لكل مجلد على حدة إن كنت متأكدًا أنك تريد أن يتمكن المستخدمون من رؤية كامل محتويات المجلد.

- Multiview دعـم «multiviews content-negotiated»؛ هـذا الخيـار مُعطَّـل افتراضيًا لأسباب أمنية، راجع توثيق أباتشي حول هذا الخيار.

- SysLinksIfOwnerMatch اتباع الوصلات الرمزية فقط إذا كان الملف أو المجلد الهدف له نفس مالك الوصلة.

إعدادات httpd

يشرح هذا القسم بعض إعدادات ضبط عفريت httpd الأساسية.

- التعليمة LockFile: تضبط التعليمة LockFile المسار إلى ملف القفل الذي سيستخدم عندما يُبنى الخادوم مع أحد الخيارين USE_FCNTL_SERIALIZED_ACCEPT أو USE_FLOCK_SERIALAIZED_ACCEPT؛ يجب أن يكون الملف مخزنًا على قرصٍ محلي، ويجب أن يترك لقيمته الافتراضية ما لم يكن مجلد السجلات موجودًا على مشاركة NFS، إذا كانت هذه هي الحالة، فيجب أن تبدَّل القيمة إلى مسار في القرص المحلي، وإلى مجلد قابل للقراءة من المستخدم الجذر (root) فقط.

- التعليمة PidFile: التعليمة PidFile تضبط الملف الذي يُسجِّل فيه الخادوم رقم عمليته (process ID أو pid اختصارًا)؛ يجب أن يكون هذا الملف قابلًا للقراءة فقط من الجذر، وفي أغلب الحالات، يجب أن تترك هذه التعليمة بقيمتها الافتراضية.

- التعليمة User: تَضبُط التعليمة User معرِّف userid المستعمل من الخادوم للإجابة عن الطلبيات؛ هذا الخيار يُعرِّف حدود وصول الخادوم، لن يتمكن زوار الموقع من الوصول إلى أي ملف لا يمكن لهذا المستخدم الوصول إليه، القيمة الافتراضية لهذه التعليمة هي "www-data".

تحذير: ما لم تكن متأكدًا تمامًا مما تفعل، فلا تضبط التعليمة User إلى root، سيسبب استخدام الجذر كمستخدم هنا في إنشاء ثغرات كبيرة في خادوم الويب.

- التعليمة Group: التعليمة Group شبيهة بالتعليمة User، التعليمة Group تحدد المجموعة التي سيجيب عبرها الخادوم عن الطلبيات؛ المجموعة الافتراضية هي "www-data" أيضًا.

وحدات أباتشي

أباتشي هو خادوم يعتمد على الوحدات، هذا يعني أن الوظيفة الأساسية فقط هي مضمَّنة في أساس الخادوم؛ الميزات الإضافية متوفرة عبر وحدات يمكن تحميلها إلى أباتشي؛ تُضمَّن افتراضيًّا مجموعة أساسية من الوحدات في الخادوم أثناء البناء، إذا بُنِي الخادوم ليستخدم الوحدات المُحمَّلة ديناميكيًا، فيمكن بناء تلك الوحدات بناءً منفصلًا ويمكن أن تضاف في أي وقت باستخدام التعليمة LoadModule؛ عدا ذلك، فيجب إعادة بناء أباتشي في كل مرة تُضاف أو تُحذف فيها الوحدات.

يبني أوبنتو أباتشي ليسمح بالتحميل الديناميكي للوحدات؛ يمكن أن تُضاف تعليمات الضبط شرطيًّا في حال تطلب وجود وحدة معينة بوضعها في قسم <IfModule>.

تستطيع تثبيت وحدات أباتشي إضافية واستخدامها في خادوم الويب؛ على سبيل المثال، نفِّذ الأمر الآتي من الطرفية لتثبيت وحدة الاستيثاق الخاصة بقواعد بيانات MySQL:

```
sudo apt-get install libapache2-mod-auth-mysql
```

انظر إلى مجلد /etc/apache2/mods-available للمزيد من الوحدات.

استخدم الأداة a2enmod لتفعيل وحدة:

```
sudo a2enmod auth_mysql
sudo service apache2 restart
```

وبشكلٍ مشابه، الأداة a2dismod ستعطل وحدة:

```
sudo a2dismod auth_mysql
sudo service apache2 restart
```

ضبط HTTPS

تُضيف الوحدة mod_ssl ميزةً مهمةً لخادوم أباتشي، ألا وهي القدرة على تشفير الاتصالات؛ وهذا يعني أنه عندما يتواصل متصفح الويب باستخدام SSL، فستُستخدَم السابقة https:// في بداية URL في شريط العنوان في المتصفح.

تتوفر الوحدة mod_ssl في الحزمة apache2-common؛ نفِّذ الأمر الآتي من الطرفية لتفعيل وحدة mod_ssl:

```
sudo a2enmod ssl
```

هنالك ملف ضبط HTTPS افتراضي في /etc/apache2/sites-available/default-ssl.conf؛ ولكي يستطيع أباتشي توفير HTTPS، فيجب توفير شهادة ومفتاح أيضًا؛ ضبط HTTPS الافتراضي سيستخدم شهادة ومفتاح مولد من الحزمة ssl-cert؛ هذه الشهادات مناسبة للاختبار، لكن يجب استبدال الشهادة والمفتاح المولد تلقائيًا بشهادة خاصة بالموقع أو الخادوم، للمزيد من المعلومات حول توليد مفتاح والحصول على شهادة، راجع «الفصل التاسع: الحماية».

أدخِل الأمر الآتي لضبط أباتشي ليتعامل مع HTTPS:

```
sudo a2ensite default-ssl
```

ملاحظة: المجلدان /etc/ssl/certs و /etc/ssl/private هما المساران الافتراضيان للشهادة والمفتاح؛ إذا ثبتت الشهادة والمفتاح في مجلد آخر، فتأكد من تغيير قيمة SSLCertificateFile و SSLCertificateKeyFile بما يلائمك.

بعد أن ضبطنا أباتشي ليستخدم HTTPS، فعلينا إعادة تشغيل الخدمة لتفعيل الإعدادات الجديدة:

```
sudo service apache2 restart
```

ملاحظة: اعتمادًا على من أين حصلت على الشهادة، ربما تحتاج إلى إدخال عبارة مرور عند تشغيل أباتشي.

تستطيع الوصول إلى صفحات الخادوم الآمنة بكتابة /https://hostname/url في شريط العنوان في المتصفح.

مشاركة إذن الكتابة

لكي يتمكن أكثر من مستخدم من الكتابة إلى نفس المجلد، فمن الضروري أن نعطي إذن الكتابة للمجموعة التي يشتركون بها؛ المثال الآتي يُشارِك إذن الكتابة للمجلد /var/www للمجموعة «webmasters»:

```
sudo chgrp -R webmasters /var/www
sudo find /var/www -type d -exec chmod g=rwxs "{}" \;
sudo find /var/www -type f -exec chmod g=rws "{}" \;
```

ملاحظة: لو أردت أن يُمنَح الوصول لأكثر من مجموعة واحدة للمجلد، ففعِّل قوائم التحكم بالوصول (ACLs).

ا. مصادر

- توثيق أباتشي، الذي يشرح بعمق معلومات حول تعليمات ضبط أباتشي، وأيضًا راجع الحزمة apache2-doc لتوثيق أباتشي الرسمي.
- راجع توثيق Mod SSL للمزيد من المعلومات المتعلقة بالوحدة SSL.
- كتاب O'Reilly المسمى «Apache Cookbook» هو مصدر رائع للقيام بضبط خاص لأباتشي.
- لأسئلة حول أباتشي على أوبنتو، فاسأل في قناة IRC المسماة #ubuntu-server على خادوم freenode.net.
- لما كان أباتشي يُدمَج عادةً مع PHP و MySQL، فصفحة ويكي أوبنتو «Apache MySQL PHP» هي مصدر جيد للمعلومات.

٢. لغة PHP5

إن PHP هي لغة برمجة عامة ملائمة لتطوير الويب؛ يمكن تضمين سكربت PHP في HTML؛ وهذا القسم سيشرح كيفية تثبيت وضبط PHP5 على خادوم أوبنتو مع أباتشي و MySQL.

يفترض هذا القسم أنك ثبتت وضبطت خادوم الويب أباتشي وقواعد بيانات MySQL؛ تستطيع الرجوع إلى الأقسام التي تشرح ضبط أباتشي و MySQL في هذا الكتاب لمزيدٍ من المعلومات.

ا. التثبيت

لغة PHP5 متوفرة في أوبنتو، وعلى عكس بايثون وبيرل المثبتتين في النظام افتراضيًّا، يجب تثبيت PHP يدويًّا.

أدخِل الأمر الآتي في الطرفية لتثبيت PHP5:

```
sudo apt-get install php5 libapache2-mod-php5
```

تستطيع تشغيل سكربتات PHP5 من سطر الأوامر؛ يجب عليك تثبيت الحزمة php5-cli لتنفيذ سكربتات PHP5 من سطر الأوامر؛ وذلك بإدخال الأمر الآتي في الطرفية:

```
sudo apt-get install php5-cli
```

تستطيع أيضًا تشغيل سكربتات PHP5 دون تثبيت وحدة PHP5 التابعة لأباتشي؛ للقيام بذلك، عليك تثبيت الحزمة php5-cgi؛ وذلك بإدخال الأمر الآتي في الطرفية:

```
sudo apt-get install php5-cgi
```

لاستخدام MySQL مع PHP5، فعليك تثبيت الحزمة php5-mysql، وبذلك بتنفيذ الأمر الآتي:

```
sudo apt-get install php5-mysql
```

وبشكل مشابه، لاستخدام PostgreSQL مع PHP5، فعليك تثبيت الحزمة php5-pgsql:

```
sudo apt-get install php5-pgsql
```

ب. الضبط

بعد أن تُثبِّت PHP5، تستطيع تشغيل سكربتات PHP5 من متصفح الويب، وإذا ثبتت الحزمة php5-cli فتستطيع تشغيل سكربتات php5 من سطر الأوامر.

خادوم أباتشي مضبوطٌ افتراضيًا لتشغيل سكربتات PHP5؛ بكلمات أخرى، وحدة PHP5 مفعَّلة افتراضيًا في خادوم أباتشي بعد تثبيت الوحدة مباشرةً؛ رجاءً تأكد إذا كانت الملفات /etc/apache2/mods/enabled/php5.conf و /etc/apache2/modsenabled/php5.l oad موجودةً، إن لم تكن موجودةً، فتستطيع تفعيل الوحدة باستخدام الأمر a2enmod.

بعد أن تثبت الحزمة المتعلقة بلغة PHP5 وتُفعِّل وحدة أباتشي، فعليك أن تعيد تشغيل خادوم أباتشي لتستطيع تنفيذ سكربتات PHP5؛ وذلك بالأمر الآتي:

```
sudo service apache2 restart
```

ج. الاختبار

للتأكد من التثبيت الصحيح للغة PHP؛ فنفِّذ سكربت phpinfo الآتي:

```
<?php
    phpinfo();
?>
```

عليك حفظ محتويات الملف السابق باسم phpinfo.php ووضعه تحت مجلد DocumentRoot في خادوم ويب أباتشي؛ وعندما توجه متصفحك نحو http://hostname/phpinfo.php فسوف يعرض لك إعدادات ضبط PHP5 المختلفة.

د. مصادر

- لتفاصيل أكثر، راجع توثيق موقع php.net.
- هنالك مجموعة كبيرة من الكتب عن PHP، كتابان جيدان من O'Reilly هما «Learning PHP»، و «PHP CookBook».

٣. خادوم Squid الوسيط

إن Squid هو خادوم تخزين وسيط للويب (web proxy cache server) الذي يوفر خدمات الوساطة والتخزين لبروتوكول نقل النص الفائق (HTTP)، وبروتوكول نقل الملفات (FTP)، وغيرهما من بروتوكولات الشبكة الشهيرة؛ يمكن أن يدعم Squid التخزين والوساطة لطلبات طبقة المقابس الآمنة (SSL) وتخزين طلبيات DNS؛ ويدعم Squid أيضًا بروتوكولات تخزين مخبأ مختلفة، مثل بروتوكول تخزين الإنترنت (Internet Cache Protocol اختصارًا ICP)، وبروتوكول تخزين النص الفائق (Hyper Text Caching Protocol اختصارًا HTCP)، وبروتوكول تخزين مصفوفة التوجيه (Cache Array Routing Protocol اختصارًا CARP)، وبروتوكول تنسيق تخزين الويب (Web Cache Coordination Protocol اختصارًا WCCP).

إن الخادوم الوسيط Squid هو حل ممتاز لاحتياجاتٍ كثيرةً للوساطة أو التخزين المؤقت، والتوسع من مكتب فرعي إلى شبكة الشركة الكبيرة وذلك بتوفير آليات مراقبة وتحكم في الوصول للمعاملات المهمة باستخدام بروتوكول إدارة الشبكة المبسط (Simple Network Management Protocol اختصارًا SNMP).

عند اختيار حاسوب ليعمل كخادوم Squid، فتأكد أنه مضبوط مع كمية كبيرة من الذاكرة الفيزيائية، حيث يستخدم Squid التخزين في الذاكرة لزيادة الأداء.

أ. التثبيت

أدخِل الأمر الآتي في الطرفية لتثبيت خادوم Squid:

```
sudo apt-get install squid3
```

ب. الضبط

يُضبَط Squid بتعديل التعليمات الموجودة ضمن ملف الضبط /etc/squid3/squid.conf؛ الأمثلة الآتية تعرض بعض التعليمات التي يمكن تعديلها لتغيير سلوك خادوم Squid؛ للمزيد من التفاصيل المعمَّقة حول Squid، فانظر إلى قسم المصادر.

تنويه: قبل تعديل ملف الضبط، تأكد أنك ستُنشِئ نسخةً من الملف الأصلي وتحميها من الكتابة كي تحصل على الإعدادات الافتراضية كمرجعٍ لك، أو أن تعيد استخدامها وقت الحاجة.

انسخ الملف /etc/squid/squid.conf واحمهِ من الكتابة بإدخال الأوامر الآتية في الطرفية:

```
sudo cp /etc/squid3/squid.conf /etc/squid3/squid.conf.original
sudo chmod a-w /etc/squid3/squid.conf.original
```

لضبط خادوم Squid لكي يستمع إلى منفذ TCP ذو الرقم ٨٨٨٨ بدلًا من منفذ TCP الافتراضي ٣١٢٨، فعدِّل التعليمة http_port كما يلي:

```
http_port 8888
```

عدِّل التعليمة visible_hostname لكي تعطي خادوم Squid اسم مضيف خاص به؛ هذا الاسم لا يفترض أن يكون نفس اسم المضيف للحاسوب؛ ضُبِطَ في هذا المثال إلى weezie:

```
visible_hostname weezie
```

باستخدام التحكم في الوصول الخاص بخادوم Squid، ربما تضبط استخدام خدمات الإنترنت التي يكون فيها Squid وسيطًا لتتوفر للمستخدمين الذي يملكون عناوين IP معيّنة؛ ففي هذا المثال، سنسمح بالوصول لمستخدمي الشبكة الفرعية 192.168.42.0/24 فقط:

أضف ما يلي إلى نهاية قسم ACL من ملف ضبط /etc/squid3/squid.conf:

```
acl fortytwo_network src 192.168.42.0/24
```

ثم أضف ما يلي إلى بداية قسم http_access في ملف /etc/squid3/squid.conf:

```
http_access allow fortytwo_network
```

باستخدام ميزات التحكم بالوصول الممتازة التي يوفرها Squid؛ فربما تضبط استخدام خدمات الإنترنت التي يكون فيها Squid وسيطًا كي تتوفر فقط أثناء ساعات العمل العادية؛ على سبيل المثال، سنحاكي وصول الموظفين خلال ساعات العمل من 9:00AM إلى 5:00PM ومن الاثنين إلى الجمعة، الذين يستخدمون الشبكة الفرعية 10.1.42.0/42:

أضف ما يلي إلى نهاية قسم ACL في ملف /etc/squid3/squid.conf:

```
acl biz_network src 10.1.42.0/24
acl biz_hours time M T W T F 9:00-17:00
```

ثم أضف ما يلي إلى أعلى قسم http_access في ملف /etc/squid3/squid.conf:

```
http_access allow biz_network biz_hours
```

ملاحظة: بعد عمل تغيرات إلى ملف الضبط /etc/squid3/squid.conf، فاحفظ الملف ثم أعد تشغيل خادوم Squid لكي تأخذ التغيرات مجراها بإدخال الأمر الآتي في الطرفية:
sudo service squid3 restart

ج. مصادر

- موقع Squid.
- صفحة ويكي أوبنتو «Squid».

٤. إطار عمل Ruby on Rails

إن Ruby on Rails هو إطار عمل مفتوح المصدر للويب لتطوير تطبيقات ويب يعتمد على قواعد البيانات؛ حيث يُفضِّل هذا الإطار المبدأ «convention over configuration».

ا. التثبيت

قبل تثبيت Ruby on Rails، يجب أن يكون لديك خادومي أباتشي و MySQL؛ رجاءً عُد للأقسام التي تشرح تثبيتهما للمزيد من المعلومات.

بعد أن تُثبَّت حزم أباتشي و MySQL؛ فيجب أن تكون جاهزًا لتثبيت حزمة Ruby on Rails؛ وذلك بإدخال الأمر الآتي في الطرفية:

```
sudo apt-get install rails
```

ب. الضبط

عدِّل ملف الضبط /etc/apache2/sites-available/000-default.conf لإعداد النطاقات.

أول شيء يجب تغييره هو التعليمة DocumentRoot:

```
DocumentRoot /path/to/rails/application/public
```

ثم عدِّل التعليمة <Directory "/path/to/rails/application/public">:

```
<Directory "/path/to/rails/application/public">
           Options Indexes FollowSymLinks MultiViews ExecCGI
           AllowOverride All
           Order allow,deny
           allow from all
           AddHandler cgi-script .cgi
</Directory>
```

يجب أن تُفعِّل الوحدة mod_rewrite لأباتشي، وذلك بإدخال الأمر الآتي في الطرفية:

```
sudo a2enmod rewrite
```

في النهاية، يجب أن تُعدِّل ملكية /path/to/rails/application/public و /path/to/rails/application/tmp للمستخدم الذي يُشغِّل عملية أباتشي:

```
sudo chown -R www-data:www-data \
/path/to/rails/application/public
sudo chown -R www-data:www-data /path/to/rails/application/tmp
```

هذا كل ما في الأمر! يجب أن يكون خادومك جاهزًا الآن لتخديم تطبيقات Ruby on Rails.

ج. مصادر

- راجع موقع Ruby on Rails لمزيدٍ من المعلومات.
- Agile Development with Rails هو مصدر رائع قد تستفيد منه.
- صفحة ويكي أوبنتو «Ruby on Rails».

٥. خادوم أباتشي Tomcat

إن أباتشي تومكات (Apache Tomcat) هو «حاوية ويب» (web container) يسمح لك بتخديم Java Servlets و JSP (Java Server Pages).

في أوبنتو دعمٌ لإصدارَيّ تومكات ٦ و ٧، حيث تومكات ٦ هي النسخة القديمة؛ وتومكات ٧ هي النسخة الحالية التي تضاف إليها الميزات الجديدة. يُعتَبَر أن كلا الإصدارين مستقر، لكن هذا الكتاب سيركز على تومكات ٧، لكن أغلبية تفاصيل الضبط المشروحة هنا صالحة لكلا النسختين.

تَدعم حزم تومكات في أوبنتو طريقتين مختلفتين لتشغيل تومكات؛ يمكنك تثبيته بالطريقة الكلاسيكية لعموم النظام، مما يجعل تومكات يبدأ في وقت الإقلاع وسيعمل كمستخدم tomcat7 (أو tomcat6) بدون امتيازات؛ لكنك تستطيع إنشاء نسخ خاصة منه وتشغيلها بامتيازات المستخدم، الذي يمكنك بدؤه أو إيقافه بنفسك؛ الطريقة الثانية هي مفيدة خصوصًا في الخادوم التطويري حيث يحتاج عدّة مستخدمين إلى اختبار البرمجيات في نسخ تومكات الخاصة بهم.

أ. التثبيت لعموم النظام

عليك إدخال الأمر الآتي في الطرفية لتثبيت خادوم تومكات:

```
sudo apt-get install tomcat7
```

الأمر السابق سيُثبِّت خادوم تومكات مع تطبيق الويب الافتراضي ROOT؛ الذي يُظهِر صفحةً بسيطةً تحتوي على "It works".

ب. الضبط

ملفات ضبط تومكات موجودة في /etc/tomcat7، بعض تعديلات الضبط الشائعة ستُشرَح هنا فقط؛ رجاءً راجع توثيق Tomcat 7.0 للمزيد.

تغيير المنافذ الافتراضية

يعمل تومكات ٧.٠ افتراضيًا بواصل HTTP (HTTP connector) على المنفذ ٨٠٨٠ وواصل AJP على المنفذ ٨٠٠٩؛ ربما تريد تغيير هذين المنفذين الافتراضيين لتفادي التضاربات مع خواديم أخرى على النظام، يمكن فعل ذلك بتعديل الأسطر الآتية في /etc/tomcat7/server.xml:

```
<Connector port="8080" protocol="HTTP/1.1"
                connectionTimeout="20000"
                redirectPort="8443" />
...
<Connector port="8009" protocol="AJP/1.3"
redirectPort="8443" />
```

تبديل JVM المُستخدَمة

يعمل تومكات افتراضيًا عملًا ممتازًا مع OpenJDK، ثم سيُجرِّب JVM الخاصة بشركة Sun؛ ثم سيجرب JVMs الأخرى؛ إذا كان لديك عدّة JVMs مثبتةً، فيمكنك ضبط أيٌّ منها سيستخدم عبر JAVA_HOME في /etc/default/tomcat7:

```
JAVA_HOME=/usr/lib/jvm/java-6-sun
```

تعريف المستخدمين وأدوارهم

يمكن أن تُعرَّف أسماء المستخدمين وكلمات مرورهم وأدوارهم (المجموعات) في حاوية Servlet؛ يتم ذلك في ملف /etc/tomcat7/tomcat-users.xml:

```
<role rolename="admin"/>
<user username="tomcat" password="s3cret" roles="admin"/>
```

ج. استخدام تطبيقات الويب القياسية التابعة لتومكات

يأتي تومكات مع تطبيقات ويب يمكن تثبيتها لأغراض التوثيق أو الإدارة أو لأغراض تجريبية.

توثيق تومكات

تحتوي الحزمة tomcat7-docs على توثيق تومكات محزمًا كتطبيق ويب تستطيع الدخول إليه افتراضيًا عبر http://server:8080/docs، وتستطيع تثبيت تلك الحزمة بالأمر الآتي:

```
sudo apt-get install tomcat7-docs
```

تطبيقات الويب لإدارة تومكات

تحتوي الحزمة tomcat7-admin على تطبيقَيّ ويب تستطيع استخدامهما لإدارة خادوم تومكات عبر واجهة ويب، يمكنك تثبيتهما عبر إدخال الأمر الآتي في الطرفية:

```
sudo apt-get install tomcat7-admin
```

أولهما هو تطبيق الويب «manager»؛ الذي يمكن الوصول إليه افتراضيًا عبر http://server:8080/manager/html؛ ويُستخدَم للحصول على حالة الخادوم وإعادة تشغيل تطبيقات الويب.

ملاحظة: الوصول إلى تطبيق manager محميٌ افتراضيًا: عليك أن تُعرِّف مستخدمًا بدور «manager-gui» في /etc/tomcat7/tomcat-users.xml قبل الوصول إليه.

التطبيق الآخر هو «host-manager» الذي يمكن الوصول إليه افتراضيًّا عبر http://server:8080/host-manager/html، ويمكن أن يُستخدَم لإنشاء مضيفين وهميين ديناميكيًّا.

ملاحظة: الوصول إلى تطبيق host-manager محميٌ افتراضيًا أيضًا: عليك أن تُعرِّف مستخدمًا بدور «admin-gui» في /etc/tomcat7/tomcat-users.xml قبل الوصول إليه.

لأسباب تتعلق بالحماية، لا يمكن للمستخدم tomcat7 أن يكتب إلى مجلد /etc/tomcat7 افتراضيًا؛ بعض الميزات في تطبيقات الويب هذه (نشر التطبيقات، أو إنشاء مضيف وهمي) تحتاج إلى إذن الكتابة إلى ذاك المجلد؛ إذا أردت استخدام هذه الميزات، فعليك تنفيذ الأوامر الآتية لإعطاء المستخدمين في مجموعة tomcat7 الامتيازات اللازمة:

```
sudo chgrp -R tomcat7 /etc/tomcat7
sudo chmod -R g+w /etc/tomcat7
```

تطبيقات ويب تومكات للتجربة

تحتوي حزمة tomcat7-example على تطبيقَيّ ويب يُستخدمان لاختبار أو شرح ميزات Servlets و JSP؛ تستطيع الوصول إليهما افتراضيًا عبر http://server:8080/examples؛ يمكنك تثبيتهما بالأمر:

```
sudo apt-get install tomcat7-examples
```

د. استخدام نسخ خاصة

يُستخدم تومكات استخدامًا واسعًا في التطوير وحالات الاختبار حيث لا يكون استخدام نسخة واحدة لعموم النظام كافيًا لعدة مستخدمين على نظام واحد؛ تأتي حزم تومكات في أوبنتو مع الأدوات اللازمة لإنشاء نسخ موجهة للمستخدمين، مما يسمح لكل مستخدم في النظام بتشغيل (دون امتيازات الجذر) نسخة خاصة منفصلة بينما ما تزال تستخدم تلك النسخة المكتبات المثبتة على النظام.

ملاحظة: من الممكن تشغيل نسخة لعموم النظام، ونسخ خاصة على التوازي (أي معًا)؛ شريطة ألّا يستخدموا نفس منافذ TCP.

تثبيت دعم النسخ الخاصة

يمكنك تثبيت كل ما يلزم لدعم النسخ الخاصة بتنفيذ الأمر الآتي في الطرفية:

```
sudo apt-get install tomcat7-user
```

إنشاء نسخة خاصة

يمكنك إنشاء مجلد لنسخة خاصة بإدخال الأمر الآتي في الطرفية:

```
tomcat7-instance-create my-instance
```

سيُنشِئ الأمر السابق مجلد my-instance جديد مع كل المجلدات الفرعية والسكربتات اللازمة؛ يمكنك على سبيل المثال تثبيت المكتبات الشائعة في المجلد الفرعي /lib ووضع تطبيق الويب في مجلد /webapps؛ لا توجد أيّة تطبيقات ويب افتراضيًا.

ضبط نسختك الخاصة

ستجد ملفات ضبط تومكات التقليدية في النسخة الخاصة في المجلد الفرعي /conf؛ يجب عليك، على سبيل المثال، تعديل ملف conf/server.xml لتغيير المنفذ الافتراضي المُستخدَم من نسخة تومكات الخاصة لتفادي التضارب مع النسخ الأخرى التي قد تكون تعمل على النظام.

بدء أو إيقاف النسخة الخاصة

يمكنك بدء نسختك الخاصة بإدخال الأمر الآتي في الطرفية (بفرض أن نسختك موجودةٌ في مجلد my-instance):

```
my-instance/bin/startup.sh
```

ملاحظة: عليك التحقق من المجلد الفرعي /logs لأي خطأ؛ إذا حصلت على خطأ java.net.BindException: Address already in use<null>:8080 فاعلم أن المنفذ مُستخدَم من قبل وعليك تغييره.

يمكنك إيقاف نسختك الخاصة بتنفيذ الأمر الآتي في سطر الأوامر:

```
my-instance/bin/shutdown.sh
```

٥. مصادر

- راجع موقع Apache Tomcat لمزيدٍ من المعلومات.
- كتاب «Tomcat: The Definitive Guide» مصدر جيد لبناء تطبيقات الويب مع تومكات.
- راجع قائمة «Tomcat Books» لمزيدٍ من الكتب.

١٢

قواعد البيانات

توفر أوبنتو خادومَيّ قواعد بيانات شهيرَين هما:

- قواعد بيانات MySQL.
- قواعد بيانات PostgreSQL.

حيث تتوفران في المستودع الرئيسي (main)؛ ويشرح هذا الفصل كيفية تثبيت وضبط خادومَي قواعد البيانات آنفَيّ الذكر.

ا. خادوم MySQL

إن MySQL هو خادوم قواعد بيانات سريع ومتعدد الخيوط (multi-threaded) ومتعدد المستخدمين ومرن جدًا؛ مُطوَّر للأنظمة الإنتاجية المحورية والتي تتحمل حِملًا ثقيلًا، ويمكن أيضًا تضمينه في البرمجيات سريعة النشر (mass-deployed).

ا. التثبيت

نفذّ الأمر الآتي في الطرفية لتثبيت MySQL:

```
sudo apt-get install mysql-server
```

سيُطلب منك إدخال كلمة مرور للمستخدم الجذر لخادوم MySQL أثناء التثبيت.

بعد أن ينتهي التثبيت، فيجب أن يبدأ خادوم MySQL تلقائيًا؛ تستطيع تنفيذ الأمر الآتي في الطرفية للتحقق إذا كان خادوم MySQL يعمل أم لا:

```
sudo netstat -tap | grep mysql
```

يجب أن تشاهد شيئًا شبيهًا بما يلي بعد تنفيذ الأمر السابق:

```
tcp    0    0    localhost:mysql    *:*    LISTEN    2556/mysqld
```

إذا لم يكن يعمل الخادوم، فتستطيع تشغيله بالأمر:

```
sudo service mysql restart
```

ب. الضبط

تستطيع تعديل الملف /etc/mysql/my.cnf لضبط الإعدادات الأساسية، مثل ملف السجل، ورقم المنفذ ... إلخ. فمثلًا لضبط MySQL ليستمع إلى الاتصالات من مضيفي الشبكة، عليك تعديل قيمة التعليمة bind-address إلى عنوان IP للخادوم:

```
bind-address    =    192.168.0.5
```

ملاحظة: عدِّل 192.168.0.5 إلى العنوان الملائم.

بعد إجراء التعديلات على ملف /etc/mysql/my.cnf؛ فيجب إعادة تشغيل عفريت MySQL:

```
sudo service mysql restart
```

أدخل الأمر الآتي في الطرفية إذا رغبت بتغيير كلمة مرور المستخدم الجذر (root) في MySQL:

```
sudo dpkg-reconfigure mysql-server-5.5
```

سيُوقَف عمل عفريت MySQL، وستُسأل عن كلمة المرور الجديدة.

ج. محركات قاعدة البيانات

على الرغم من أن الضبط الافتراضي لخادوم MySQL الموفر من حزم أوبنتو يعمل عملًا صحيحًا دون مشاكل، لكن هنالك بعض الأمور التي عليك أخذها بعين الاعتبار قبل الإكمال.

صُمِّمَت قواعد بيانات MySQL للسماح بتخزين البيانات بطرقٍ مختلفة؛ يُشار لهذه الطرق إما بمحركات قواعد البيانات أو محركات التخزين (Storage engine)؛ هنالك محركان رئيسيان ستكون مهتمًا بهما: InnoDB و MyISAM؛ لا تتغير طريقة التعامل مع محركات التخزين المختلفة بالنسبة للمستخدم النهائي؛ حيث تتعامل MySQL مع الأمور بطريقة مختلفة وراء الستار، أي أنه بغض النظر عن محرك التخزين الذي تستخدمه، فإنك ستتعامل مع قواعد البيانات بنفس الطريقة تمامًا.

لكل محرك إيجابياته وسلبياته؛ وبينما من الممكن دمج عدّة محركات قواعد بيانات على مستوى الجدول، لكن ذلك خطيرٌ، فربما يقلل ذلك من الفعالية والأداء لأنك تُقسِّم الموارد بين محركين بدلًا من تخصيصها لمحرك واحد فقط.

المحـرك MyISAM هـو الأقـدم بيـن المحركيـن المـذكورين؛ يمكـن أن يكـون أسـرع مـن InnoDB في حالات معيّنة ويفضل الأعمال التي تتطلب القراءة فقط؛ تتمحور بعض تطبيقات الويب حول MyISAM (على الرغم أنها لن تُبطَئ إذا استخدمت InnoDB)؛ يدعم MyISAM أيضًا نوع البيانات FULLTEXT؛ الذي يسمح بالبحث بسرعة كبيرة في كمياتٍ كبيرةٍ من النص؛ لكن MyISAM قادر على قفل الجدول بأكمله فقط عند الكتابة، هذا يعني أن عمليةً واحدةً فقط تستطيع تحديث الجدول في لحظة زمنية معيّنة؛ قد يكون هذا إعاقةً لتوسع تطبيق يعتمد على هـذا الجـدول؛ ولا يحتـوي MyISAM علـى ميـزة «journaling»، وهـذا يعنـي أنـه مـن الصـعب استرجاع البيانات بعد حدوث انهيار؛ المقال الآتي يوفر بعض النقاط لاعتبارها حول استخدام MyISAM في قاعدة بيانات إنتاجية.

المحـرك InnoDB هـو محـرك قواعـد بيانـات أكثر حداثةً، صُمّم ليكون متوافقًا مع ACID الذي يضمن إجراء العمليات على قواعد البيانات بطريقة عملية؛ قفل الكتابة يحـدث علـى مسـتوى السجل (row) ضمن الجدول؛ هذا يعني أنه من الممكن إجراء عدّة تحديثات لسجلات جدولٍ ما في نفس الوقت؛ التخزين الموقت للبيانات يحدث في الذاكرة ضمن محرك قواعد البيانات، مما يسمح بالتخزين على أساس السجل وليس على أساس كتلة الملف (file block)؛ ولكي يتوافق مع ACID، فإن كل العمليات تحدث بطريقة «journaled» مستقلةً عن الجداول الرئيسـية؛ وهـذا يؤدي إلى استرجاع البيانات استرجاعًا عمليًا.

إن InnoDB هو المحرك الافتراضي في MySQL 5.5 ومن المستحسن بشدة استخدامه بدلًا من MyISAM ما لم تكن تريد استخدام مزايا خاصة بذاك المحرك.

د. الضبط المتقدم

إنشاء ملف ضبط my.cnf

هنالك عدد من المعاملات التي يمكن تعديلها في ملف ضبط MySQL مما يسمح لك بتحسين أداء الخادوم مع مرور الوقت؛ ربما تجد الأداة «Percona's my.cnf generating tool» مفيدةً للإعداد الابتدائي؛ ستولد هذه الأداة ملف my.cnf ليكون أكثر ملائمةً لإمكانيات ومتطلبات خادومك.

لا تستبدل ملف my.cnf المولد من Percona إذا وضعت بيانات في قاعدة بيانات، بعض التغييرات في الملف لن تسبب مشاكل لأنها تُعدِّل طريقة تخزين البيانات على القرص الصلب ولن تتمكن من تشغيل MySQL؛ إذا أردت استخدامه وكانت لديك بيانات موجودة مسبقًا، فعليك أن تجري mysqldump ثم تعيد التحميل:

```
mysqldump --all-databases --all-routines -u root \
-p > ~/fulldump.sql
```

ستُسأل عن كلمة مرور المستخدم الجذر لقواعد MySQL قبل إنشاء نسخة من البيانات؛ من المستحسن أن تتأكد أنه لا يوجد مستخدمين أو عمليات تستخدم قاعدة البيانات قبل إجراء هذه الخطوة؛ ربما تأخذ عملية النسخ بعض الوقت بناءً على مقدار البيانات الموجودة في قاعدة البيانات لديك؛ لن ترى شيئًا على الشاشة أثناء تنفيذ الأمر السابق.

أغلق خادوم MySQL بعد إكمال عملية التفريغ (dump):

```
sudo service mysql stop
```

خذ الآن نسخةً احتياطيةً من my.cnf واستبدله بالملف الجديد:

```
sudo cp /etc/my.cnf /etc/my.cnf.backup
sudo cp /path/to/new/my.cnf /etc/my.cnf
```

الآن احذف وأعد تهيئة مجال قواعد البيانات وتأكد أن الملكية صحيحة قبل إعادة تشغيل MySQL:

```
sudo rm -rf /var/lib/mysql/*
sudo mysql_install_db
sudo chown -R mysql: /var/lib/mysql
sudo service start mysql
```

كل ما تبقى الآن هو إعادة استيراد بياناتك؛ وللحصول على فكرة عن مدى إتمام عملية الاستيراد، فربما تجد الأداة pv (Pipe Viewer) مفيدةً؛ الأمر الآتي يظهر كيفية تثبيت واستخدام pv لهذه الحالة، ربما لا تريد أن تستخدمها وكل ما عليك فعله هو استبدال pv بالأمر cat؛ تجاهل أية أوقات متوقعة للانتهاء (ETA) مولدة من pv؛ لأنها مبنية على الوقت المستغرق لكي يُعالَج كل سجل من الملف، لكن سرعة إدراج البيانات قد تختلف اختلافًا كبيرًا من سجل إلى سجل:

```
sudo apt-get install pv
pv ~/fulldump.sql | mysql
```

ملاحظة: هذا ليس ضروريًا لكل تعديلات my.cnf؛ أغلبية المتغيرات التي قد ترغب في تعديلها لتحسين الأداء يمكن أن تُغيَّر حتى وإن كان يعمل الخادوم؛ تأكد من الحصول على نسخة احتياطية من ملفات الضبط والبيانات قبل إجراء التعديلات.

الأداة MySQL Tuner

الأداة «MySQL Tuner» هي أداة مفيدة تستطيع الاتصال إلى خدمة MySQL التي تعمل وتوفر اقتراحات عن كيفية ضبطها بأفضل ضبط لحالتك؛ وكما كان يعمل الخادوم لوقتٍ أطول، كلما كانت «النصيحة» التي سيوفرها mysqltuner أفضل؛ خذ بعين الاعتبار الانتظار لمدة ٢٤ ساعة في بيئة إنتاجية قبل تشغيل هذه الأداة؛ تستطيع تثبيت mysqltuner من مستودعات أوبنتو:

```
sudo apt-get install mysqltuner
```

ثم تشغيلها بعد تثبيتها بالأمر:

```
mysqltuner
```

وانتظر التقرير النهائي، سيوفر القسم العلوي معلوماتٍ عن خادوم قاعدة البيانات، ويوفر القسم السفلي اقتراحاتٍ لكي تعدلها في ملف my.cnf؛ يمكن تعديل أغلبية الاقتراحات على الخادوم مباشرةً دون إعادة تشغيله، انظر إلى توثيق MySQL الرسمي للمتغيرات المناسبة لتعديلها في البيئات الإنتاجية.ما يلي هو جزء من تقرير من قاعدة بيانات إنتاجية الذي يُظهِر أن هنالك بعض الفائدة من زيادة مقدار ذاكرة تخزين الطلبية:

```
-------- Recommendations -----------------------------
General recommendations:
     Run OPTIMIZE TABLE to defragment tables for better
performance
     Increase table_cache gradually to avoid file descriptor
limits
```

```
Variables to adjust:
      key_buffer_size (> 1.4G)
      query_cache_size (> 32M)
      table_cache (> 64)
      innodb_buffer_pool_size (>= 22G)
```

تعليق أخير عن ضبط قواعد البيانات: بينما نستطيع أن نقول أن بعض الإعدادات هي الأفضل، لكن قد يختلف الأداء من تطبيق لآخر؛ على سبيل المثال، ما يعمل عملًا ممتازًا لوردبريس (Wordpress) قد لا يكون الأفضل لدروبال (Drupal) أو جوملا (Joomla) أو التطبيقات التجارية؛ الأداء متعلقٌ بأنواع الطلبيات واستخدام الفهارس، وإذا ما كان تصميم قاعدة البيانات جيدًا، وهكذا… ربما من الجيد إنفاق بعض الوقت في البحث عن إعدادات ملائمة لقواعد البيانات بناءً على التطبيقات التي تستخدمها؛ لكن بعد أن تتجاوز التعديلات حدًا معيّنًا، فإن أيّة تغييرات تجريها لا تتسبب إلا بتحسين بسيط جدًا في أداء التطبيق، ومن الأفضل لك تحسين التطبيق نفسه، أو التفكير في توسيع خادوم MySQL إما باستخدام عتاد أفضل أو بإضافة خواديم تابعة (Slaves).

٥. مصادر

- راجع الموقع الرئيسي لقواعد MySQL لمزيدٍ من المعلومات.
- التوثيق الكامل متوفر بصيغ online و offline من «MySQL Developers portal».
- لمعلومات عامة حول SQL، انظر إلى كتاب «Using SQL Special Edition».
- صفحة ويكي أوبنتو «Apache MySQL PHP» فيها بعض المعلومات المفيدة.

٢. خادوم PostgreSQL

PostgreSQL هي قاعدة بيانات علائقية تعتمد على الكائنات وتملك ميزات أنظمة قواعد البيانات التجارية التقليدية مع تحسينات موجودة في الجيل الجديد من أنظمة DBMS.

ا. التثبيت

أدخل الأمر الآتي في الطرفية لتثبيت PostgreSQL:

```
sudo apt-get install postgresql
```

بعد انتهاء التثبيت، عليك ضبط خادوم PostgreSQL بناءً على متطلباتك، على الرغم من أن الضبط الافتراضي قابل للاستخدام.

ب. الضبط

الاتصال عبر TCP/IP معطَّل افتراضيًا؛ تدعم PostgreSQL عدّة طرق للاستيثاق من العميل؛ طريقة الاستيثاق IDENT تُستعمَل للمستخدمين المحليين ولمستخدم postgres ما لم يُضبَط غير ذلك؛ رجاءً راجع «PostgreSQL Administrator's Guide» إذا أردت ضبط بدائل مثل Kerberos.

سنفترض في ما يلي أنك ستُفعِّل اتصالات TCP/IP وتستخدم طريقة MD5 للاستيثاق من العميل؛ تُخزَّن ملفات ضبط PostgreSQL في المجلد /etc/postgresql/<version>/main؛ على سبيل المثال، إذا ثبتت خادوم PostgreSQL 9.1، فإن ملفات الضبط ستُخزَّن في المجلد /etc/postgresql/9.1/main.

تنويه: لضبط الاستيثاق بطريقة ident، فأضف مدخلات إلى /etc/postgresql/9.1/main/pg_ident.conf؛ هنالك تعليقات تفصيلية في الملف لتساعدك.

لتفعيل اتصالات TCP/IP، عليك تعديل الملف /etc/postgresql/9.1/main/postgresql.conf ومن ثم تحديد السطر 'localhost' = listen_addresses# ثم تغييره إلى:

```
listen_addresses = '*'
```

ملاحظة: للسماح باتصالات IPv4 و IPv6، استبدل "localhost" بالرمز "::".

ربما تريد تعديل بقية المعاملات، إذا كنت تعرف ماذا تفعل للتفاصيل، ارجع إلى ملف الضبط أو إلى توثيق PostgreSQL.

الآن وبعد أن استطعنا الاتصال بخادوم PostgreSQL فإن الخطوة الآتية هي ضبط كلمة مرور للمستخدم postgres؛ نفذ الأمر الآتي في الطرفية للاتصال بقاعدة بيانات PostgreSQL الافتراضية:

```
sudo -u postgres psql template1
```

يتصل الأمر السابق بقاعدة بيانات PostgreSQL المسماة template1 كالمستخدم postgres؛ بعد أن تتصل إلى خادوم PostgreSQL وتحصل على مِحَث لإدخال تعليمات SQL.

يمكنك إدخال أمر SQL الآتي في مِحَث psql لضبط كلمة المرور للمستخدم postgres:

```
ALTER USER postgres with encrypted password 'your_password';
```

بعد ضبط كلمة المرور، عدِّل الملف /etc/postgresql/9.1/main/pg_hba.conf لاستخدام استيثاق MD5 مع المستخدم postgres:

```
local       all       postgres       md5
```

في النهاية، يجب أن تُعيد تشغيل خدمة PostgreSQL لتهيئة الضبط الجديد، وذلك بإدخال الأمر الآتي من الطرفية:

```
sudo service postgresql restart
```

تحذير: الضبط السابق ليس كاملًا بأي شكل من الأشكال، رجاءً راجع «PostgreSQL Administrator's Guide» لمعاملات ضبط إضافية.

يمكنك اختبار اتصالات الخادوم من الأجهزة الأخرى باستخدام عملاء PostgreSQL:

```
sudo apt-get install postgresql-client
psql -h postgres.example.com -U postgres -W
```

ملاحظة: استبدل اسم النطاق في المثال السابق باسم نطاقك الفعلي.

ج. مصادر

- كما ذُكِر سابقًا، فإن «PostgreSQL Administrator's Guide» هو مصدر رائع، وهو متوفر أيضًا في حزمة postgresql-doc-9.1؛ نفذ ما يلي لتثبيت تلك الحزمة:

```
sudo apt-get install postgresql-doc-9.1
```

أدخِل الوصلة file:///usr/share/doc/postgresql-doc-9.1/html/index.html في شريط العنوان في متصفحك لمشاهدة الدليل.

- راجع أيضًا صفحة ويكي أوبنتو «PostgreSQL» لمزيدٍ من المعلومات.



تطبيقات LAMP



تثبيت LAMP (الذي هو Linux + Apache + MySQL + PHP/Perl/Python) هو إعداد شائع لخواديم أوبنتو؛ هنالك تشكيلة واسعة جدًا من البرمجيات مفتوحة المصدر المكتوبة لتجميعة برامج LAMP؛ أشهر تلك البرمجيات هي تطبيقات الويكي، وأنظمة إدارة المحتوى، وبرمجيات الإدارة مثل phpMyAdmin.

ميزة من مزايا LAMP هي المرونة غير العادية لاستخدام قواعد بيانات أو خواديم ويب أو لغات برمجية مختلفة بدائل شائعة لقواعد MySQL تتضمن PostgreSQL و SQLite؛ وتُستخدَم Python أو Perl أو Ruby بدلًا من PHP؛ ويَستبدل Nginx أو Cherokee أو Lighttpd الخادوم أباتشي.

أسرع طريقة للبدء في تثبيت LAMP هي استخدام tasksel؛ الأداة tasksel هي أداة خاصة بدبيان/أوبنتو التي تُثبّت حزمًا مترابطة للقيام «بمهمة» في نظامك؛ أدخِل الأمر الأتي في الطرفية لتثبيت خادوم LAMP:

```
sudo tasksel install lamp-server
```

بعد إتمام عملية التثبيت، ستكون قادرًا على تثبيت أغلبية تطبيقات LAMP بهذه الطريقة:

- تنزيل أرشيف يحتوي على الملفات المصدرية للتطبيق.
- استخراج الملفات من الأرشيف إلى مجلد يمكن لخادوم الويب الوصول إليه.
- اعتمادًا على المكان الذي استخرجت الملفات إليه، فاضبط خادوم الويب ليُخدِّم الصفحات من هناك.
- اضبط التطبيق للاتصال بقاعدة البيانات.

- شغِّل سكربتًا، أو افتح صفحةً من التطبيق لتثبيت قاعدة البيانات التي يحتاج لها هذا التطبيق.
- بعد أن أجريت الخطوات السابقة أو خطواتٍ شبيهةٍ بها، فأنت جاهزٌ الآن للبدء باستعماله.

عيب من عيوب هذه الطريقة هي أن ملفات التطبيق لا توضع في مكان قياسي في نظام الملفات، الأمر الذي قد يسبب فوضى؛ عيب آخر كبير هو تحديث التطبيق، فعند إصدار نسخة جديدة منه، فيجب إجراء نفس عملية تثبيت التطبيق لتحديثه.

لحسن الحظ، هنالك عدد من تطبيقات LAMP مُحزَّمة في أوبنتو، ومتوفرة للتثبيت كغيرها من التطبيقات؛ لكن حسب التطبيق، فربما هنالك خطوات أخرى للضبط والإعداد؛ سيشرح هذا الفصل تثبيت بعض تطبيقات LAMP.

ا. تطبيق Moin Moin

إن MoinMoin هو محرك ويكي مكتوب بلغة بايثون ومبني على محرك الويكي PikiPiki ومرخص برخصة GUN GPL.

ا. التثبيت

نفِّذ الأمر الآتي لتثبيت MoinMoin:

```
sudo apt-get install python-moinmoin
```

يجب أن تكون قد ثبتت خادوم أباتشي؛ رجاءً راجع «الفصل الحادي عشر» لمزيدٍ من المعلومات حول تثبيت أباتشي.

ب. الضبط

لضبط أول تطبيق ويكي خاص بك، فعليك تنفيذ سلسلة الأوامر الآتية؛ على فرض أنك تُنشِئ «ويكي» باسم mywiki:

```
cd /usr/share/moin
sudo mkdir mywiki
sudo cp -R data mywiki
sudo cp -R underlay mywiki
sudo cp server/moin.cgi mywiki
sudo chown -R www-data.www-data mywiki
sudo chmod -R ug+rwX mywiki
sudo chmod -R o-rwx mywiki
```

يجـــب الآن أن تضـــبط MoinMoin لكـــي يـــرى الـــويكي الجديـــد mywiki؛ لضـــبط MoinMoin، افتح الملف /etc/moin/mywiki.py وعدِّل السطر الآتي:

```
data_dir = '/org/mywiki/data'
```

إلى:

```
data_dir = '/usr/share/moin/mywiki/data'
```

أيضًا، تحت الخيار data_dir، أضف الخيار data_underlay_dir:

```
data_underlay_dir='/usr/share/moin/mywiki/underlay'
```

ملاحظة: إذا لم يكن الملف /etc/moin/mywiki.py موجودًا، فعليك نسخ /usr/share/moin/config/wikifarm/mywiki.py إلى /etc/moin/mywiki.py ثم تنفيذ التغيير المذكور آنفًا.

ملاحظة: إذا سميت الويكي باسم my_wiki_name، فيجب إضافة السطر ("my_wiki_name",r".*") إلى ملف /etc/moin/farmconfig.py بعد السطر ("mywiki", r".*").

بعد أن تضبط MoinMoin ليعثر على أول تطبيق ويكي mywiki عليك ضبط أباتشي وجعله جاهزًا لتطبيق الويكي.

يجب أن تُضيف الأسطر الآتية في ملف /etc/apache2/sites-available/default ضمن الوسم

```
<VirtualHost *>:
### moin
    ScriptAlias /mywiki "/usr/share/moin/mywiki/moin.cgi"
    alias /moin_static193 "/usr/share/moin/htdocs"
    <Directory /usr/share/moin/htdocs>
    Order allow,deny
    allow from all
    </Directory>
### end moin
```

بعد أن تضبط خادوم أباتشي وتجعله جاهزًا لتطبيق الويكي، يجب عليك أن تعيد تشغيله، وذلك بإدخال الأمر الآتي لإعادة تشغيل خادوم أباتشي:

```
sudo service apache2 restart
```

ج. التجربة

للتأكد من عمل تطبيق الويكي، وجِّه متصفحك للوصلة الآتية:

```
http://localhost/mywiki
```

للمزيد من المعلومات، راجع موقع MoinMoin الرسمي.

د. مصادر

- للمزيد من المعلومات انظر إلى ويكي «moinmoin».
- أيضًا، صفحة ويكي أوبنتو «MoinMoin».

٢. تطبيق MediaWiki

إن MediaWiki هـي برمجيـة Wiki مبنيـة علـى الـويب مكتوبـة بلغـة PHP؛ يمكنهـا أن تستخدم نظام إدارة قواعد بيانات MySQL أو PostgreSQL.

ا. التثبيت

قبـل تثـبيت MediaWiki، يجـب عليـك تثـبيت أباتشـي ولغـة برمجـة PHP5 ونظـام إدارة قواعـد بيانات؛ وأشـهرها MySQL أو PostgreSQL، اختـر واحـدًا بنـاءً علـى احتياجاتـك، رجـاءً ارجع إلى الأقسام التي تشرح تثبيتها في هذا الكتاب للمزيد من المعلومات.

نفِّذ الأمر الآتي في الطرفية لتثبيت MediaWiki:

```
sudo apt-get install mediawiki php5-gd
```

لوظائف MediaWiki إضافية، انظر إلى الحزمة mediawiki-extensions.

ب. الضبط

ملـف ضـبط أباتشـي mediawiki.conf مثبَّـتٌ فـي /etc/apache2/conf-available/، يجب عليك إزالة التعليق من السطر الآتي للوصول إلى تطبيق MediaWiki:

```
# Alias /mediawiki /var/lib/mediawiki
```

بعد أن تُزيل التعليق من السطر السابق، ففعّل الضبط ثم أعد تشغيل خادوم أباتشي ثم ادخل إلى MediaWiki عبر الرابط الآتي http://localhost/mediawiki/config/index.php:

```
sudo a2enconf mediawiki.conf
sudo service apache2 restart
```

تنويه: رجاءً اقرأ القسم «...Checking environment» في تلك الصفحة؛ ستكون قادرًا على حل مشاكل عديدة بقراءة هذا القسم بحذر.

بعد إكمال الضبط، يجب عليك أن تنقل الملف LocalSettings.php إلى المجلد /etc/mediawiki:

```
sudo mv /var/lib/mediawiki/config/LocalSettings.php \
/etc/mediawiki/
```

ربما تريد أيضًا تعديل /etc/mediawiki/LocalSettings.php لكي تضبط حد الذاكرة الأقصى (معطّل افتراضيًا):

```
ini_set( 'memory_limit', '64M' );
```

ج. الإضافات

توفّر الإضافات ميزات وتحسينات على تطبيق MediaWiki؛ تمنح هذه الإضافات مدراء الويكي والمستخدمين النهائيين القدرة على تخصيص MediaWiki لتناسب احتياجاتهم.

يمكنك تنزيل إضافات MediaWiki كأرشيف أو عبر سحبها (checkout) من مستودع Subversion؛ عليك أن تنسخها إلى مجلد /var/lig/mediawiki/extensions/؛ يجب عليك أيضًا إضافة السطر الآتي في نهاية الملف /etc/mediawiki/LocalSettings.php:

```
require_once "$IP/extensions/ExtentionName/ExtentionName.php";
```

د. مصادر

- للمزيد من المعلومات، رجاءً راجع موقع MediaWiki.
- يحتوي كتاب «MediaWiki Administrators’ Tutorial Guide» على معلوماتٍ قيمة لمدراء MediaWiki الجدد.
- صفحة ويكي أوبنتو «MediaWiki» هي مصدرٌ جيدٌ أيضًا.

٣. تطبيق phpMyAdmin

إن phpMyAdmin هو تطبيق LAMP مكتوب خصيصًا لإدارة خواديم MySQL، وهو مبرمج بلغة PHP، ويمكن الوصول إليه عبر متصفح الويب، حيث يوفِّر phpMyAdmin واجهة رسومية لمهام إدارة قواعد البيانات.

ا. التثبيت

قبل تثبيت phpMyAdmin فستحتاج إلى وصول إلى قاعدة بيانات MySQL سواءً على نفس المضيف الذي سيُثبَّت عليه phpMyAdmin أو على مضيف آخر متوفر عبر الشبكة؛ للمزيد من المعلومات حول MySQL فانظر إلى القسم الخاص بها في هذا الكتاب؛ أدخِل الأمر الآتي لتثبيت phpMyAdmin:

```
sudo apt-get install phpmyadmin
```

ستظهر لك نافذة لاختيار أي خادوم ويب سيُضبَط ليستخدمه phpMyAdmin؛ سنستخدم لبقية هذا القسم خادوم أباتشي كخادوم ويب.

في المتصفح، اذهب إلى http://server/phpmyadmin مستبدلًا server باسم مضيف الخادوم الحقيقي؛ وعند صفحة تسجيل الدخول، اكتب root في حقل اسم المستخدم، أو أي مستخدم MySQL إذا كنت قد أعددت واحدًا؛ ثم أدخل كلمة مرور ذاك المستخدم.

بعد تسجيل الدخول، تستطيع إعادة ضبط كلمة مرور الجذر إن كان ذلك ضروريًا، وإنشاء المستخدمين، وإنشاء أو حذف قواعد البيانات والجداول ...إلخ.

ب. الضبط

ملفات الضبط الخاصة ببرمجية phpMyAdmin موجودةٌ في مجلد /etc/phpmyadmin؛ ملف الضبط الرئيسي هو /etc/phpmyadmin/config.inc.php يحتوي هذا الملف خيارات الضبط التي تُطبَّق عمومًا على phpMyAdmin.

لاستخدام phpMyAdmin لإدارة قواعد بيانات MySQL على خادوم آخر، عدِّل قيمة ما يلي في ملف /etc/phpmyadmin/config.inc.php:

```
$cfg['Servers'][$i]['host'] = 'db_server';
```

ملاحظة: استبدل db_server باسم مضيف الخادوم البعيد أو عنوان IP الخاص به؛ أيضًا تأكد أن مضيف phpMyAdmin لديه الأذونات الكافية للوصول إلى قاعدة البيانات البعيدة.

بعد ضبطه، سجل خروجك من phpMyAdmin ثم أعد تسجيل الدخول، ويجب أن تستطيع الوصول إلى الخادوم الجديد.

الملفان config.header.inc.php و config.footer.inc.php يستخدمان لإضافة ترويسة وتذييل HTML إلى phpMyAdmin.

ملف ضبط آخر مهم هو /etc/phpmyadmin/apache.conf، توجد وصلة رمزية لهذا الملف في /etc/apache2/conf.d/phpmyadmin.conf ويُستخدَم لضبط أباتشي لتخديم صفحات phpMyAdmin؛ يحتوي هذا الملف على تعليمات لتحميل PHP، وأذونات المجلد ...إلخ.

ج. مصادر

- يـأتي توثيـق phpMyAdmin مثبتًـا مـع الحزمـة ويمكـن الوصـول إليـه مـن وصـلة «phpMyAdmin Documentation» تحت شعار phpMyAdmin؛ يمكن الوصول إلى التوثيق الرسمي أيضًا في موقع phpMyAdmin.
- كتاب «Mastering phpMyAdmin» هو مصدر جيد للمعلومات.
- مصدر ثالث هو صفحة ويكي أوبنتو «phpMyAdmin».

٤. تطبيق Wordpress

إن وردبريس (Wordpress) هي أداة تدوين، ومنصة نشر، ونظام إدارة محتوى مكتوبة بلغة PHP ومرخصة برخصة GNU GPLv2.

ا. التثبيت

نفِّذ الأمر الآتي في سطر الأوامر لتثبيت وردبريس:

```
sudo apt-get install wordpress
```

يجب عليك أيضًا تثبيت خادوم أباتشي وخادوم MySQL؛ راجع الأقسام التي تُعنى بتثبيتهما وإعدادهما في هذا الكتاب.

ب. الضبط

لضبط أول تطبيق وردبريس، فعليك ضبط موقع أباتشي؛ افتح الملف /etc/apache2/sites-available/wordpress.conf وضع فيه الأسطر الآتية:

```
Alias /blog /usr/share/wordpress
<Directory /usr/share/wordpress>
   Options FollowSymLinks
   AllowOverride Limit Options FileInfo
   DirectoryIndex index.php
   Order allow,deny
   Allow from all
</Directory>
<Directory /usr/share/wordpress/wp-content>
   Options FollowSymLinks
   Order allow,deny
   Allow from all
</Directory>
```

ثم فعّل الموقع الجديد:

```
sudo a2ensite wordpress
```

بعد أن انتهيت من ضبط خادوم أباتشي، وجعلته جاهزًا لتطبيق ووردبريس، فعليك الآن إعادة تشغيله وذلك بتنفيذ الأمر الآتي:

```
sudo service apache2 restart
```

لتبسيط تشغيل عدّة نسخ من ووردبريس، فسمّ ملف الضبط بناءً على اسم المضيف؛ وهذا يعني أنك تستطيع أن تملك عدّة مضيفين وهميين بمطابقة اسم المضيف في ملف الضبط مع ملف اسم المضيف الوهمي في أباتشي؛ فعلى سبيل المثال، تكون أسماء الملفات هي ‎/etc/wordpress/config-10.211.55.50.php، أو قد تكون على سبيل المثال: ‎/etc/wordpress/config-hostalias1.php ... إلخ.

هذه التعليمات تفترض أنك تستطيع الوصول إلى أباتشي عبر المضيف المحلي (ربما باستخدام نفق SSH)؛ إذا لم يكن ذلك هو الأمر، فاستبدل ‎/etc/wordpress/config-localhost.php بالاسم ‎/etc/wordpress/config/NAME_OF_VIRTUAL_HOST.php.

بعد أن يُكتَب ملف الضبط، فعليك اختيار نمط لأسماء مستخدمي MySQL وكلمات مرورهم لكل نسخة ووردبريس؛ لكن سنعرض في هذا الكتاب مثال واحد هو localhost فقط.

علينا الآن ضبط ووردبريس لاستخدام قاعدة بيانات MySQL؛ افتح الملف /etc/wordpress/config-localhost.php واكتب الأسطر الآتية:

```
<?php
define('DB_NAME', 'wordpress');
define('DB_USER', 'wordpress');
define('DB_PASSWORD', 'yourpasswordhere');
define('DB_HOST', 'localhost');
define('WP_CONTENT_DIR', '/usr/share/wordpress/wp-content');
?>
```

ثم أنشِئ قاعدة البيانات، وذلك بفتح ملف مؤقت باسم wordpree.sql فيه أوامر MySQL الآتية:

```
CREATE DATABASE wordpress;
GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,DROP,ALTER
ON wordpress.*
TO wordpress@localhost
IDENTIFIED BY 'yourpasswordhere';
FLUSH PRIVILEGES;
```

نفِّذ أوامر MySQL السابقة بالأمر:

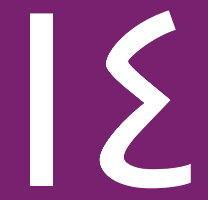
```
cat wordpress.sql | sudo mysql \
--defaults-extra-file=/etc/mysql/debian.cnf
```

يجب أن تكون نسخة ووردبريس عندك قابلة للضبط بزيارة الوصلة http://localhost/blog/wp-admin/install.php، ثم اكتب اسم الموقع واسم المستخدم وكلمة المرور وبريدك الإلكتروني ثم اضغط على «تثبيت ووردبريس».

لاحظ كلمة المرور المُولَّدة إن لم تختر واحدةً، ثم سجِّل دخولك إلى لوحة تحكم وبرديس.

ج. مصادر

- توثيق Wordpress.org Codex.
- صفحة ويكي أوبنتو المسماة «WordPress».



خواديم الملفات



إذا كان لديك أكثر من حاسوب في نفس الشبكة، فعند حدٍّ معيَّن ستحتاج إلى مشاركة الملفات بين تلك الحواسيب؛ نشرح في هذا الفصل تثبيت وضبط FTP، و NFS، و CUPS.

١. خادوم FTP

بروتوكول نقل الملفات (File Transfer Protocol اختصارًا FTP) هو بروتوكول TCP لتنزيل الملفات بين الحواسيب؛ في الماضي، كان يُستخدم أيضًا لرفع الملفات، لكن هذه الطريقة لا توفر إمكانية التشفير، وستُنقَل معلومات المستخدم مع البيانات في صيغة سهلة التفسير؛ إذا كنت تبحث هنا عن طريقة آمنة لرفع أو تنزيل الملفات، فألقِ نظرةً على قسم OpenSSH في الفصل السادس.

يعمل FTP وفق نمط «عميل/خادوم»؛ حيث تُسمى مكونة FTP في الخادوم «عفريت FTP»، الذي يستمع بشكل متواصل لطلبات FTP من العملاء البعيدين؛ وعند وصول طلب، فإنه يجري عملية الدخول ويُهيّء الاتصال، وستُنفَّذ الأوامر المُرسَلة من عميل FTP أثناء مدة عمل الجلسة.

يمكن الوصول إلى خادوم FTP بإحدى الطريقتين:

- مستخدم مجهول.
- مستخدم موثوق.

في نمط المستخدم المجهول (Anonymous)؛ يمكن للعملاء البعيدين الوصول إلى خادوم FTP بحساب المستخدم الافتراضي المُسمى «anonymous» أو «ftp» ويرسلون عنوان بريد إلكتروني ككلمة مرور؛ أما في نمط المستخدم الموثوق، فيجب على المستخدم امتلاك حساب وكلمة مرور؛ الخيار الثاني غير آمن أبدًا ولا يجب أن يستخدم إلا في الحالات الخاصة؛

إذا كنت تبحث عن طريقة آمنة لنقل الملفات، فانظر إلى SFTP في OpenSSH-Server. وصول المستخدم إلى مجلدات وملفات خادوم FTP يتعلق بالأذونات المعطية للحساب أثناء تسجيل الدخول؛ وكقاعدة عامة، سيخفي عفريت FTP المجلد الجذر لخادوم FTP وسيحول المستخدم إلى مجلد منزل FTP؛ وهذا سيخفي بقية نظام الملفات من الجلسات البعيدة.

ا. تثبيت خادوم FTP «vsftpd»

إن vsftpd هو عفريت FTP متوفر في أوبنتو، ومن السهل تثبيته وإعداده وصيانته؛ لتثبيت vsftpd، عليك تنفيذ الأمر الآتي في الطرفية:

```
sudo apt-get install vsftpd
```

ب. ضبط الوصول المجهول لخادوم FTP

افتراضيًا، لم يُضبَط vsftpd للسماح للمستخدمين المجهولين بالتنزيل؛ إذا كنت تريد السماح لهم بالتنزيل، فعدِّل الملف /etc/vsftpd.conf مغيّرًا:

```
anonymous_enable=Yes
```

سيُنشَأ مستخدم باسم ftp مع مجلد المنزل /srv/ftp أثناء التثبيت؛ هذا هو مجلد FTP الافتراضي.

إذا أردت تغيير هذا المسار إلى /srv/files/ftp على سبيل المثال، فببساطة أنشِئ مجلدًا في مكانٍ آخر، وغيّر مجلد المنزل للمستخدم ftp:

```
sudo mkdir /srv/files/ftp
sudo usermod -d /srv/files/ftp
```

أعد تشغيل الخدمة vsftpd بعد عمل التغيرات السابقة:

```
sudo restart vsftpd
```

في النهاية، انسخ أيّة ملفات ومجلدات تريد للمستخدمين المجهولين تنزيلها عبر ftp إلى /srv/files/ftp أو إلى /srv/ftp إذا أبقيت على الإعدادات الافتراضية.

ج. ضبط FTP للاستيثاق من المستخدمين

افتراضيًا، يكون vsftpd مضبوطًا على الاستيثاق من مستخدمي النظام والسماح لهم بتنزيل الملفات؛ إذا أردت السماح للمستخدمين برفع الملفات، فعدِّل الملف /etc/vsftpd.conf:

```
write_enable=YES
```

ثم أعد تشغيل vsftpd:

```
sudo restart vsftpd
```

الآن عندما يتصل مستخدمو النظام عبر FTP، فسيبدؤون في مجلد المنزل الخاص بهم، حيث يستطيعون تنزيل أو رفع الملفات أو إنشاء المجلدات ...إلخ.

وبشكلٍ مشابه، لا يُسمَح افتراضيًا للمستخدمين المجهولين برفع الملفات إلى خادوم FTP؛ لتغيير ذلك الإعداد عليك أن تُزيل التعليق عن السطر الآتي وتُعيد تشغيل خدمة vsftpd:

```
anon_upload_enable=YES
```

تحذير: إن السماح للمستخدمين المجهولين برفع الملفات إلى الخادوم هو أمرٌ خطيرٌ جدًا، ولا يُفضَّل أبدًا أن يُسمَح للمستخدمين المجهولين برفع الملفات مباشرةً من الإنترنت.

يحتوي ملف الضبط على العديد من خيارات الضبط؛ توجد معلومات حول كل خيار في ملف الضبط؛ ويمكنك مراجعة صفحة الدليل man 5 vsftpd.conf للمزيد من التفاصيل حول كل إعداد.

د. تأمين FTP

هنالك خيارات في /etc/vsftpd.conf للمساعدة في جعل vsftpd أكثر أمانًا؛ فمثلًا يمكن أن يقيّد وصول المستخدمين إلى مجلدات المنزل الخاصة بهم بإزالة التعليق عن السطر:

```
chroot_local_users=YES
```

يمكنك أن تقيّد قائمة محددة من المستخدمين إلى مجلدات المنزل الخاصة بهم فقط:

```
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd.chroot_list
```

بعد إزالة التعليق عن الخيارات السابقة؛ أنشِئ ملف /etc/vsftpd.chroot_list الذي يحتوي على قائمة بالمستخدمين المسموح لهم واحدًا في كل سطر؛ ثم أعد تشغيل vsftpd:

```
sudo restart vsftpd
```

يحتوي الملف /etc/ftpusers أيضًا على قائمة بالمستخدمين غير المسموح لهم بالوصول إلى FTP؛ القائمة الافتراضية تتضمن root، و daemon، و nobody …إلخ. لتعطيل الوصول إلى FTP لمستخدمين آخرين، فأضفهم ببساطة إلى القائمة.

يمكن أن يُشفَّر FTP باستخدام FTPS، الذي يختلف عن SFTP؛ FTPS هو FTP عبر طبقة المقابس الآمنة (SSL)؛ إن SFTP هو مثل جلسة FTP عبر اتصال SSH مشفر؛ اختلاف رئيسي هو أن مستخدمي SFTP يجب أن يملكوا حساب

«shell» على النظام، بدلًا من صدفة nologin؛ قد لا يكون توفير صدفة لكل المستخدمين أمرًا ملائمًا في بعض البيئات مثل خادوم ويب مشترك؛ لكن من الممكن تقييد مثل هذه الحسابات إلى SFTP فقط وتعطيل التعامل مع الصدفة، راجع قسم OpenSSH لمزيدٍ من المعلومات.

لضبط FTPS، عدِّل الملف /etc/vsftpd.conf وأضف في النهاية:

```
ssl_enable=Yes
```

أيضًا، لاحظ الخيارات المتعلقة بالشهادة والمفتاح:

```
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
```

ضُبِطَت هذه الخيارات افتراضيًا إلى الشهادة والمفتاح الموفر من الحزمة ssl-sert؛ لكن يجب استبدالهما في البيئات الإنتاجية بالشهادة والمفتاح المُولَّد لمضيف محدد؛ للمزيد من المعلومات حول الشهادات، راجع «الفصل التاسع: الحماية».

أعد الآن تشغيل vsftpd، وسيُجبر المستخدمون غير المجهولين على استخدام FTPS:

```
sudo restart vsftpd
```

للسماح للمستخدم بصدفة /usr/sbin/nologin بالوصول إلى FTP، لكن عدم امتلاك وصول للصدفة، فعدِّل ملف /etc/shells مضيفًا الصدفة nologin:

```
# /etc/shells: valid login shells
/bin/csh
/bin/sh
/usr/bin/es
/usr/bin/ksh
/bin/ksh
/usr/bin/rc
/usr/bin/tcsh
/bin/tcsh
/usr/bin/esh
/bin/dash
/bin/bash
/bin/rbash
/usr/bin/screen
/usr/sbin/nologin
```

هذا ضروريٌ لأن vsftpd يستخدم PAM افتراضيًا للاستيثاق؛ والملف /etc/pam.d/vsftpd يحتوي على:

```
auth        required        pam_shells.so
```

الصدفات التي تسمح الوحدة PAM لها بالوصول هي الصدفات المذكورة في ملف /etc/shells.

يمكن ضبط أغلبية عملاء FTP الشهيرين ليتصلوا عبر FTPS. الأداة lftp التي تعمل من سطر الأوامر لها إمكانية استخدام FTPS أيضًا.

٥. مصادر

- راجع موقع vsftpd الرسمي لمزيدٍ من المعلومات.
- لتفاصيل الخيارات في /etc/vsftpd.conf راجع صفحة دليل vsftpd.conf.

٢. نظام ملفات الشبكة NFS

يسمح NFS للنظام بمشاركة المجلدات والملفات مع الآخرين عبر الشبكة؛ إذ يمكن للمستخدمين والبرامج الوصول إلى الملفات في الأنظمة البعيدة كأنها ملفاتٌ محلية باستخدام NFS.

بعض الميزات الملحوظة التي يوفرها استخدام NFS:

- محطات العمل المحلية تستهلك مساحة قرص أقل لأنها تستخدم بيانات يمكن تخزينها على جهاز واحد وتبقى متاحةً للبقية عبر الشبكة.
- لا توجد حاجة ليُنشَأ للمستخدمين مجلدات منزل منفصلة في كل جهاز شبكي؛ حيث يمكن ضبط مجلدات المنزل على خادوم NFS وتتوفر للجميع عبر الشبكة.
- أجهزة التخزين مثل سواقات CD-ROM وأقراص USB يمكن استخدامها من الأجهزة الأخرى على الشبكة، وربما يقلل هذا من عدد مشغلات الوسائط القابلة للإزالة في الشبكة.

ا. التثبيت

أدخل الأمر الآتي في الطرفية لتثبيت خادوم NFS:

```
sudo apt-get install nfs-kernel-server
```

ب. الضبط

تستطيع ضبط المجلدات لكي «تُصدَّر» عبر إضافتها لملف /etc/exports، على سبيل المثال:

```
/ubuntu     *(ro,sync,no_root_squash)
/home       *(rw,sync,no_root_squash)
```

تستطيع استبدال علامة "*" بإحدى صيغ أسماء المضيفين، تأكد من أن تعريف اسم المضيف محدد كي لا تستطيع الأنظمة غير المعنية أن تصل إلى NFS.

نفِّذ الأمر الآتي في مِحَث الطرفية لتشغيل خادوم NFS:

```
sudo service nfs-kernel-server start
```

ج. ضبط عميل NFS

استخدم الأمر mount لوصل مجلد NFS مشترك من جهاز لآخر؛ وذلك بكتابة أمرٍ شبيه بالأمر الآتي في الطرفية:

```
sudo mount example.hostname.com:/ubuntu /local/ubuntu
```

تحذير: يجب أن تكون نقطة الوصل /local/ubuntu موجودةً مسبقًا، ولا يجب أن يكون هنالك أيّة ملفات أو مجلدات فرعية في نقطة الوصل.

طريقة أخرى لوصل مشاركة NFS من جهاز لآخر هي إضافة سطر إلى ملف /etc/fstab؛ يجب أن يُحدِّد هذا السطر اسم مضيف خادوم NFS، والمجلد الذي صُدِّرَ من الخادوم، والمجلد في الجهاز المحلي الذي يجب وصل NFS إليه؛ الشكل العام للسطر الذي سيُضاف إلى ملف /etc/fstab هو:

```
example.hostname.com:/ubuntu /local/ubuntu nfs
rsize=8192,wsize=8192,timeo=14,intr
```

إذا حدثت معك مشكلة في وصل NFS، فتأكد أن الحزمة nfs-common مثبتة في نظام عميلك؛ وذلك بإدخال الأمر الآتي في الطرفية:

```
sudo apt-get install nfs-common
```

د. مصادر

- Linux NFS faq2.
- صفحة ويكي أوبنتو «NFS Howto».

٣. مُبادر iSCSI

إن iSCSI ‏(Internet Small Computer System Interface) هو بروتوكول يسمح بنقل أوامر SCSI عبر الشبكة؛ عادةً يُستخدَم iSCSI في SAN ‏(Storage Area Network) للسماح للخواديم بالوصول إلى مخزن كبير لمساحة القرص الصلب؛ يُشير بروتوكول iSCSI للعملاء «بالمبادرين» (initiators) ولخواديم iSCSI بالأهداف (targets).

يمكن أن يُضبَط خادوم أوبنتو كمبادر أو هدف iSCSI، يوفر هذا الكتاب الأوامر والضبط اللازم لإعداد مبادر iSCSI، على فرض أنك تملك هدف iSCSI في شبكتك وتملك الامتيازات المناسبة للاتصال إليه؛ التعليمات حول إعداد هدف تختلف اختلافًا كبيرًا بين مزودي العتاد، لذلك راجع توثيق الشركة لضبط هدف iSCSI الذي عندك.

ا. تثبيت مبادر iSCSI

لضبط خادوم أوبنتو كمبادر iSCSI، فثبِّت الحزمة open-iscsi بإدخال الأمر الآتي:

```
sudo apt-get install open-iscsi
```

ب. ضبط مبادر iSCSI

بعد أن تُثبِّت حزمة open-iscsi، عليك تعديل الملف /etc/iscsi/iscsid.conf مغيرًا ما يلي:

```
node.startup = automatic
```

تستطيع التأكد إذا كان الهدف متوفرًا حاليًا باستخدام الأداة iscsiadm؛ وذلك بإدخال الأمر الآتي في الطرفية:

```
sudo iscsiadm -m discovery -t st -p 192.168.0.10
```

- m-: يحدد النمط الذي سيُنفَّذ فيه iscsiadm.
- t-: يحدد نوع الاستكشاف.
- p-: يحدد عنوان IP للهدف.

ملاحظة: عدِّل 192.168.0.10 إلى عنوان IP للهدف على شبكتك المحلية.

إذا كان الهدف متوفرًا، فيجب أن تشاهد مخرجات شبيهة بما يلي:

```
192.168.0.10:3260,1 iqn.1992-05.com.emc:sl7b92030000520000-2
```

ملاحظة: قد يختلف رقم iqn وعنوان IP في الأعلى بناءً على العتاد الذي تستخدمه.

يجب أن تكون الآن قادرًا على الاتصال بهدف iSCSI، واعتمادًا على إعدادات الهدف، فربما تحتاج لإدخال بيانات المستخدم لتسجيل الدخول إلى عقدة iSCSI:

```
sudo iscsiadm -m node --login
```

تأكد الآن أن القرص الجديد قد عُثِرَ عليه باستخدام dmesg:

```
dmesg | grep sd

[   4.322384] sd 2:0:0:0:Attached scsi generic sg1 type 0
[   4.322797] sd 2:0:0:0: [sda] 41943040 512-byte logical
blocks:(21.4GB/20.0 GiB)
[   4.322843] sd 2:0:0:0: [sda] Write Protect is off
[   4.322846] sd 2:0:0:0: [sda] Mode Sense: 03 00 00 00
[   4.322896] sd 2:0:0:0: [sda] Cache data unavailable
[   4.322899] sd 2:0:0:0: [sda] Assuming drive cache: write
through
[   4.323230] sd 2:0:0:0: [sda] Cache data unavailable
[   4.323233] sd 2:0:0:0: [sda] Assuming drive cache: write
through
[   4.325312] sda: sda1 sda2 < sda5 >
[   4.325729] sd 2:0:0:0: [sda] Cache data unavailable
[   4.325732] sd 2:0:0:0: [sda] Assuming drive cache: write
through
[   4.325735] sd 2:0:0:0: [sda] Attached SCSI disk
[2486.941805] sd 4:0:0:3: Attached scsi generic sg3 type 0
[2486.952093] sd 4:0:0:3: [sdb] 1126400000 512-byte logical
blocks: (576 GB/537GiB)
[2486.954195] sd 4:0:0:3: [sdb] Write Protect is off
[2486.954200] sd 4:0:0:3: [sdb] Mode Sense: 8f 00 00 08
[2486.954692] sd 4:0:0:3: [sdb] Write cache: disabled, read
cache: enabled, doesn't support DPO or FUA
[2486.960577] sdb: sdb1
[2486.964862] sd 4:0:0:3: [sdb] Attached SCSI disk
```

في الناتج أعلاه، يكون sdb هو قرص iSCSI الجديد؛ تذكر أن هذا مجرد مثال، قد يختلف الناتج عمّا تراه على الشاشة.

أنشِئ الآن قسمًا، وهيّء نظام الملفات، وصِل قرص iSCSI الجديد؛ وذلك بإدخال ما يلي في الطرفية:

```
sudo fdisk /dev/sdb
n
p
enter
w
```

ملاحظة: الأوامر الآتية من داخل الأداة fdisk؛ راجع man fdisk لتعليمات تفصيلية؛ أيضًا الأداة cfdisk في بعض الأحيان تكون «صديقة» للمستخدم أكثر.

هيّء الآن نظام الملفات وصِله إلى srv/ على سبيل المثال:

```
sudo mkfs.ext4 /dev/sdb1
sudo mount /dev/sdb1 /srv
```

في النهاية، أضف مدخلة إلى etc/fstab/ لوصل قرص iSCSI أثناء الإقلاع:

```
/dev/sdb1    /srvext4   defaults,auto,_netdev    0      0
```

فكرة جيدة هي التأكد أن كل شيء يعمل على ما يرام قبل إعادة تشغيل الخادوم.

ج. مصادر

- موقع Open-iSCSI الإلكتروني.
- صفحة ويكي دبيان «Open-iSCSI».

٤. خادوم الطباعة CUPS

الآلية الرئيسية للطباعة وخدمات الطباعة في أوبنتو هي «النظام الشائع للطباعة في يونكس» (Common UNIX Printing System اختصارًا CUPS)، نظام الطباعة هذا هو طبقة محمولة متوفرة مجانًا التي أصبحت المعيار القياسي الجديد للطباعة في غالبية توزيعات لينُكس.

يدير CUPS مهام الطباعة والطلبيات ويوفر خدمات طباعة عبر الشبكة باستخدام «بروتوكول الطباعة عبر الإنترنت» (Internet Printing Protocol اختصارًا IPP)، بينما يوفر CUPS دعمًا لمجالٍ واسعٍ جدًا من الطابعات، بدءًا من طابعات مصفوفة النقط (dot-matrix) إلى الطابعات الليزرية وما بينهما؛ ويدعم CUPS أيضًا «PostScript Printer Description» (PPD) والاكتشاف التلقائي لطابعات الشبكة، ويوفر واجهة ويب بسيطة كأداة للضبط والإدارة.

ا. التثبيت

أدخل الأمر الآتي في الطرفية لتثبيت CUPS:

```
sudo apt-get install cups
```

سيعمل خادوم CUPS تلقائيًا بعد نجاح التثبيت.

ولاستكشاف الأخطاء، يمكنك الوصول إلى أخطاء خادوم CUPS عبر ملف سجل في الملف /var/log/cups/error_log؛ إذا لم يُظهِر سجل الأخطاء معلوماتٍ كافيةً لحل المشاكل التي تواجهك، فيمكن زيادة درجة «الإسهاب» لسجل CUPS بتغيير التعليمة LogLevel في ملف الضبط إلى "debug" أو حتى إلى "debug2"، مما يؤدي إلى تسجيل كل شيء؛ تأكد من إعادة القيمة الافتراضية "info" بعد حل مشكلتك لتفادي زيادة حجم السجل زيادةً كبيرةً جدًا.

ب. الضبط

يُضبَط سلوك خادوم CUPS عبر تعليمات موجودة في ملف /etc/cups/cupsd.conf؛ يتبِّع ملف ضبط CUPS نفس الصيغة العامة لملف الضبط الرئيسي لخادوم أباتشي؛ سنذكر هنا بعض الأمثلة عن الإعدادات التي يمكن تغييرها.

تنويه: عليك إنشاء نسخة من الملف الأصلي قبل تعديل ملف الضبط، وعليك حماية تلك النسخة من الكتابة، لذلك ستكون لديك الإعدادات الافتراضية كمرجع أو لإعادة استخدامها وقت الحاجة.

انسخ الملف /etc/cups/cupsd.conf واحمِهِ من الكتابة بالأوامر الآتية:

```
sudo cp /etc/cups/cupsd.conf /etc/cups/cupsd.conf.original
sudo chmod a-w /etc/cups/cupsd.conf.original
```

التعليمة ServerAdmin: لضبط عنوان البريد الإلكتروني لمدير خادوم CUPS، عليك أن تُحرِّر ملف الضبط /etc/cups/cupsd.conf، ثم أضف أو عدِّل سطر ServerAdmin بما يلائمك؛ فمثلًا إن كنت أنت مدير خادوم CUPS، وكان بريدك الإلكتروني هو user@example.com، فعليك تعديل سطر ServerAdmin ليبدو كما يلي:

```
ServerAdmin user@example.com
```

التعليمة Listen: يستمع خادوم CUPS في أوبنتو افتراضيًا على بطاقة loopback فقط على عنوان IP 127.0.0.1؛ ولكي تجعل خادوم CUPS يستمع على عنوان IP لبطاقة شبكية، فعليك تحديد إما اسم مضيف، أو عنوان IP، أو اختيارًا، عنوان IP ومنفذ؛ وذلك بإضافة التعليمة Listen؛ على سبيل المثال، لو كان خادوم CUPS يقبع على شبكة محلية بعنوان IP هو 192.168.10.250 وتريد أن تجعله متاحًا لبقية الأنظمة على هذه الشبكة الفرعية؛ فعليك تعديل /etc/cups/cupsd.conf؛ وإضافة التعليمة Listen، كما يلي:

```
Listen 127.0.0.1:631                 # existing loopback Listen
Listen /var/run/cups/cups.sock       # existing socket Listen
Listen 192.168.10.250:631            # Listen on the LAN
interface, Port 631 (IPP)
```

قد تحذف أو تضع تعليقًا قبل الإشارة إلى عنوان loopback ‏(127.0.0.1) إذا لم ترغب في أن يستمع cupsd إلى هذه البطاقة لكنك تريده أن يستمع فقط إلى بطاقة إيثرنت للشبكة المحلية LAN؛ لتفعيل الاستماع لكل منافذ الشبكة بما فيها loopback لمضيف معيّن، فتستطيع إنشاء قيد Listen لاسم المضيف (socrates) كما يلي:

```
Listen socrates:631  # Listen on all interfaces for the
hostname 'socrates'
```

أو بحذف التعليمة Listen واستخدام Port عوضًا عنها:

```
Port 631  # Listen on port 631 on all interfaces
```

للمزيد من الأمثلة عن تعليمات الضبط لخادوم CUPS، راجع صفحة الدليل الخاصة بملف الضبط بإدخال الأمر الآتي:

```
man cupsd.conf
```

ملاحظة: في كل مرة تُعدِّل فيها على ملف الضبط /etc/cups/cupsd.conf؛ فستحتاج إلى إعادة تشغيل خادوم CUPS بكتابة الأمر التالي في الطرفية:

```
sudo service cups restart
```

ج. واجهة الويب

ملاحظة: يمكن أن يُضبَط ويُراقَب CUPS باستخدام واجهة ويب، التي تتوفر افتراضيًا على http://localhost:631/admin؛ يمكن استخدام واجهة الويب لإجراء كل مهام إدارة الطابعة.

لكي تنفذ المهام الإدارية عبر واجهة الويب، فعليك إما تفعيل حساب الجذر على خادومك، أو الاستيثاق كمستخدم في المجموعة lpadmin؛ ولأسبابٍ أمنية، لن يستوثق CUPS من مستخدم لا يملك كلمة مرور.

لإضافة مستخدم إلى المجموعة lpadmin، فعليك تنفيذ الأمر الآتي في الطرفية:

```
sudo usermod -aG lpadmin username
```

يتوفر توثيق في لسان Documentation/Help في واجهة الويب.

د. مصادر

- موقع CUPS الإلكتروني.

15

خدمات البريد الإلكتروني

تشترك العديد من الأنظمة في عملية الحصول على بريد إلكتروني من شخصٍ لآخر عبر الشبكة أو الإنترنت التي تعمل مع بعضها بعضًا؛ ويجب أن يُضبَط كل واحد من هذه الأنظمة ضبطًا صحيحًا لكي تتم العملية بنجاح؛ يستخدم المُرسِل «عميل مستخدم البريد» (Mail User Agent اختصارًا MUA) أو عميل بريد إلكتروني، لإرسال رسالة عبر واحد أو أكثر من «عملاء نقل البريد» (Mail Transfer Agents اختصارًا MTA)، سيسلم آخرهم البريد إلى «عميل إيصال البريد» (Mail Delivery Agent اختصارًا MDA) لإيصال البريد إلى صندوق بريد المستلم، الذي بدوره يحصل عليه عميل البريد الإلكتروني للمستلم عادةً باستخدام خادوم POP3 أو IMAP.

١. خادوم Postfix

إن Postfix هو عميل نقل البريد (MTA) الافتراضي في أوبنتو؛ الذي يُوصَف بأنه سريع وسهل الإدارة، وآمن ومتوافق مع عميل نقل البريد sendmail؛ يشرح هذا القسم طريقة تثبيت وضبط Postfix، ويشرح أيضًا كيفية إعداد خادوم SMTP باستخدام اتصال آمن (لإرسال رسائل البريد الإلكتروني بأمان).

ملاحظة: لن يشرح هذا الكتاب «Postfix Virtual Domains» للمزيد من المعلومات حول النطاقات الوهمية وغيرها من إعدادات الضبط المتقدمة، فراجع قسم «مصادر» في نهاية هذا القسم.

ا. التثبيت

نفِّذ الأمر الآتي في الطرفية لتثبيت postfix:

```
sudo apt-get install postfix
```

ستُسأل بعض الأسئلة أثناء عملية التثبيت، وسيُشرَح الضبط بتفاصيل أكبر في المرحلة القادمة.

ب. الضبط الأساسي

نفِّذ الأمر الآتي في الطرفية لضبط postfix:

```
sudo dpkg-reconfigure postfix
```

ستظهر واجهة مستخدم، اختر منها القيم الآتية على كل شاشة:

```
Internet Site
mail.example.com
steve
mail.example.com, localhost.localdomail, localhost
No
127.0.0.1/8 8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.0.0/24
0
+
all
```

ملاحظة: استبدل mail.example.com بالنطاق الذي سيقبل استلام البريد عليه، و 192.168.0.0/24 بالشبكة التي عندك ومجالها؛ و steve باسم ملائم للمستخدم.

الآن هو وقتٌ ملائمٌ لتحديد صيغة صندوق البريد التي تنوي استخدامها؛ افتراضيًا Postfix يستخدم mbox لصيغة صندوق البريد؛ وبدلًا من تعديل ملف الضبط مباشرةً، يمكنك استخدام الأمر postconf لضبط كل معاملات postfix؛ ستُخزَّن معاملات الضبط في ملف ‎/etc/postfix/main.cf؛ وإذا أردت إعادة ضبط معامل معيَّن، يمكنك إما أن تنفذ الأمر أو تعدل الملف يدويًا؛ فلضبط صيغة صندوق البريد إلى Maildir:

```
sudo postconf -e 'home_mailbox = Maildir/'
```

ملاحظة: هذا سيضع البريد الجديد في مجلد ‎/home/username/Maildir/، لذلك تريد ضبط عميل تسليم البريد (MDA) لاستخدام نفس المسار.

ج. استيثاق SMTP

يسمح SMTP-AUTH للعميل بالتعريف عن نفسه باستخدام آلية استيثاق (SASL)، يجب استخدام أمن طبقة النقل

(TLS) لتشفير عملية الاستيثاق؛ سيسمح خادوم SMTP للعميل بأن ينقل البريد بعد الاستيثاق.

لضبط Postfix مع SMTP-AUTH باستخدام SASL (Dovecot SASL):

```
sudo postconf -e 'smtpd_sasl_type = dovecot'
sudo postconf -e 'smtpd_sasl_path = private/auth-client'
sudo postconf -e 'smtpd_sasl_local_domain ='
sudo postconf -e 'smtpd_sasl_security_options = noanonymous'
sudo postconf -e 'broken_sasl_auth_clients = yes'
sudo postconf -e 'smtpd_sasl_auth_enable = yes'
sudo postconf -e 'smtpd_recipient_restrictions = \
permit_sasl_authenticated,permit_mynetworks, \
reject_unauth_destination'
```

ملاحظة: الضبط smtpd_sasl_path هو مسار نسبي إلى مجلد طلبيات Postfix.

ثم ولِّد أو احصل على شهادة TLS رقمية، راجع «الفصل التاسع: الحماية»؛ هذا المثال يستخدم أيضًا سلطة شهادات (Certificate Authority أو CA)، للمزيد من المعلومات حول ذلك، انظر إلى قسم «سلطة الشهادات».

ملاحظة: عملاء مستخدمي البريد (MUA) التي تتصل إلى خادوم البريد عبر TLS يجب أن تتعرف على الشهادة المستخدمة في TLS؛ يمكن فعل ذلك إما باستخدام شهادة من سلطة شهادات تجارية، أو استخدام شهادة موقعة ذاتيًا، وعلى المستخدمين أن يُثبِّتوا أو يقبلوا الشهادة يدويًا، شهادات TLS من عميل نقل بريد إلى عميل نقل بريد آخر لا يُتحقَّق منها إلا بعد موافقة مسبقة من المنظمات المتأثرة؛ لا يوجد سبب لعدم استخدام شهادة موقعة ذاتيًا عند استعمال TLS من MTA إلى MTA، ما لم تتطلب السياسات المحلية ذلك؛ راجع قسم «إنشاء شهادة موقعة ذاتيًا» لمزيدٍ من المعلومات.

بعد أن تحصل على الشهادة، اضبط Postfix لتوفير تشفير TLS للبريد المُرسَل والمُستلَم:

```
sudo postconf -e 'smtp_tls_security_level = may'
sudo postconf -e 'smtpd_tls_security_level = may'
sudo postconf -e 'smtp_tls_note_starttls_offer = yes'
sudo postconf -e 'smtpd_tls_key_file =
/etc/ssl/private/server.key'
sudo postconf -e 'smtpd_tls_cert_file =
/etc/ssl/certs/server.crt'
sudo postconf -e 'smtpd_tls_loglevel = 1'
sudo postconf -e 'smtpd_tls_received_header = yes'
sudo postconf -e 'myhostname = mail.example.com'
```

إذا كنت تستخدم سلطة الشهادات الخاصة بك لتوقيع الشهادة، فأدخِل:

```
sudo postconf -e 'smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem'
```

مرةً أخرى، للمزيد من المعلومات حول الشهادات، راجع الفصل التاسع.

ملاحظة: بعد تنفيذ كل الأوامر السابقة، فيكون Postfix قد ضُبِطَ ليستخدم SMTP-AUTH وشهادة موقعة ذاتيًا أُنشِئت لاتصال TLS مشفر.

```
# See /usr/share/postfix/main.cf.dist for a commented, more
complete
# version

smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h
```

```
myhostname = server1.example.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = server1.example.com, localhost.example.com,
localhost
relayhost =
mynetworks = 127.0.0.0/8
mailbox_command = procmail -a "$EXTENSION"
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
smtpd_sasl_local_domain =
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_recipient_restrictions =
permit_sasl_authenticated,permit_mynetworks,reject
_unauth_destination
smtpd_tls_auth_only = no
smtp_tls_security_level = may
smtpd_tls_security_level = may
smtp_tls_note_starttls_offer = yes
smtpd_tls_key_file = /etc/ssl/private/smtpd.key
smtpd_tls_cert_file = /etc/ssl/certs/smtpd.crt
smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom
```

بعد إكمال الضبط الابتدائي لخدمة postfix؛ فنفذ الأمر الآتي لإعادة تشغيل العفريت:

```
sudo service postfix restart
```

يـدعم Postfix اسـتخدام SMTP-AUTH كما هو معرَّف فـي RFC2554؛ الذي هو مبني على SASL؛ لكنه يبقى ضروريًا إعداد استيثاق SASL قبل استخدام SMTP-AUTH.

د. ضبط SASL

يـدعم Postfix نسـختين مـن SASL همـا Cyrus SASL و Dovecot SASL؛ لتفعيـل Dovecot SASL، فيجـب تثبيت حزمـة dovecot-common، وذلك بإدخـال الأمر الآتـي من الطرفية:

```
sudo apt-get install dovecot-common
```

يجب تعديل ملف الضبط /etc/dovecot/conf.d/10-master.conf؛ مغيِّرًا ما يلي:

```
service auth {
    # auth_socket_path points to this userdb socket by default.
It's typically
    # used by dovecot-lda, doveadm, possibly imap process, etc.
Its default
    # permissions make it readable only by root, but you may
need to relax these
    # permissions. Users that have access to this socket are
able to get a list
    # of all usernames and get results of everyone's userdb
lookups.
    unix_listener auth-userdb {
        #mode = 0600
        #user =
        #group =
    }
    # Postfix smtp-auth
    unix_listener /var/spool/postfix/private/auth {
        mode = 0660
        user = postfix
        group = postfix
    }
```

ولكي نسمح لعملاء Outlook باستخدام SMTP-AUTH، فعدِّل السطر الآتي في قسم authentication mechanisms في ملف /etc/dovecot/conf.d/10-auth.conf:

```
auth_mechanisms = plain
```

إلى ما يلي:

```
auth_mechanisms = plain login
```

بعد أن ضَبَطتَ Dovecot، فأعد تشغيله بالأمر:

```
sudo service dovecot restart
```

ه. تفعيل Mail-Stack Delivery

خيار آخر لضبط Postfix لاستعمال SMTP-AUTH هو استخدام الحزمة mail-stack-delivery (كانت تُحزَّم مسبقًا باسم dovecot-postfix)؛ هذه الحزمة ستُثبِّت Dovecot وتضبط Postfix ليستخدمها لاستيثاق SASL وعميل تسليم البريد (MDA)؛ تضبط هذه الحزمة Dovecot أيضًا للخدمات IMAP و IMAPS و POP3 و POP3S.

ملاحظة: ربما تريد أو لا تريد تشغيل IMAP، أو IMAPS، أو POP3، أو POP3S على خادوم البريد عندك؛ على سبيل المثال، إذا كنت تضبط خادومك ليكون بوابةً للبريد، أو مُرَشِّحًا للرسائل العشوائية (Spam) أو الفيروسات ...إلخ. فإذا كانت هذه هي الحالة عندك، فمن الأسهل استخدام الأوامر السابقة لضبط Postfix لاستخدام SMTP-AUTH.

لتثبيت الحزمة، أدخِل ما يلي في الطرفية:

```
sudo apt-get install mail-stack-delivery
```

يجب أن تحصل الآن على خادوم بريد يعمل تمامًا؛ لكن هنالك بعض الخيارات التي تريد ضبطها لمزيدٍ من التخصيص؛ على سبيل المثال، تستخدم الحزمة السابقة شهادة ومفتاح من حزمة ssl-cert، وفي بيئة إنتاجية يجب أن تستخدم شهادة ومفتاح مولّد للمضيف؛ راجع قسم «الشهادات» لمزيدٍ من التفاصيل.

عدّل الخيارات الآتية في /etc/postfix/main.cf بعد أن تخصص الشهادة والمفتاح للمضيف:

```
smtpd_tls_cert_file = /etc/ssl/certs/ssl-mail.pem
smtpd_tls_key_file = /etc/ssl/private/ssl-mail.key
```

ثم أعد تشغيل Postfix:

```
sudo service postfix restart
```

و. الاختبار

اكتمل الآن ضبط SMTP-AUTH؛ حان الآن الوقت لاختبار الإعدادات.

للتأكد إذا كان SMTP-AUTH و TLS يعملان عملًا صحيحًا، فنفِّذ الأمر الآتي:

```
telnet mail.example.com 25
```

بعد أن تُنشِئ اتصالًا لخادوم البريد postfix، اكتب ما يلي:

```
ehlo mail.example.com
```

إذا رأيت الأسطر الآتية بين غيرها، فإن كل شيء يعمل على ما يرام؛ اكتب quit للخروج.

```
250-STARTTLS
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
250 8BITMIME
```

ز. استكشاف الأخطاء وإصلاحها

سنقدم في هذا القسم بعض الطرق الشائعة لتحديد السبب إذا حدثت مشكلة ما.

الخروج من chroot

ستُثبَّت الحزمة postfix في أوبنتو افتراضيًا في بيئة «chroot» لأسبابٍ أمنية؛ يمكن أن يزيد هذا من تعقيد إصلاح المشاكل.

لتعطيل عمل chroot، حدد السطر الآتي في ملف /etc/postfix/master.cf:

```
smtp      inet  n     -     -     -     -     smtpd
```

وعدِّله كما يلي:

```
smtp      inet  n     -     n     -     -     smtpd
```

تحتاج إلى إعادة تشغيل Postfix لاستخدام الضبط الجديد، وذلك بإدخال الأمر الآتي في الطرفية:

```
sudo service postfix restart
```

تفعيل Smtps

إذا احتجت إلى smtps، فعدِّل الملف /etc/postfix/master.cf وأزل التعليق عن السطر الآتي:

```
smtps     inet  n       -       -       -       -       smtpd
   -o smtpd_tls_wrappermode=yes
   -o smtpd_sasl_auth_enable=yes
   -o
smtpd_client_restrictions=permit_sasl_authenticated,reject
   -o milter_macro_daemon_name=ORIGINATING
```

ملفات السجل

يُرسِل Postfix جميع رسائل السجل إلى ملف /var/log/mail.log، لكن يمكن أن تضيع رسائل الخطأ والتحذير في السجل العادي، لذلك فإنها تُسجَّل أيضًا إلى /var/log/mail.err و /var/log/mail.warn على التوالي وبالترتيب.

لمراقبة الرسائل الداخلة إلى السجل في الوقت الحقيقي، فاستخدم الأمر tail مع الخيار -f كما يلي:

```
tail -f /var/log/mail.err
```

يمكن زيادة كمية التفاصيل التي ستُسجَّل؛ هذه بعض خيارات الضبط لزيادة مستوى التسجيل لبعض «المناطق» المذكورة أعلاه.

لزيادة نشاط تسجيل TLS، فاضبط الخيار smtpd_tls_loglevel إلى قيمة من ١ إلى ٤:

```
sudo postconf -e 'smtpd_tls_loglevel = 4'
```

إذا كانت لديك مشكلة في إرسال أو استقبل البريد من نطاق معين، فيمكنك إضافة ذاك النطاق إلى معامل debug_peer_list:

```
sudo postconf -e 'debug_peer_list = problem.domain'
```

يمكنك زيادة درجة الإسهاب لأي عملية تابعة لعفريت Postfix بتعديل الملف/etc/postfix /master.cf وبإضافة الخيار v- بعد القيد، على سبيل المثال، عدِّل القيد smtp كما يلي:

```
smtp      unix  -       -       -       -       -       smtp -v
```

ملاحظة: من الضروري ملاحظة أنه بعد إنشاء تعديل من تعديلات التسجيل المذكورة آنفًا، فيجب أن يعاد تحميل عملية Postfix لكي تُدرِك الضبط الجديد:

```
sudo service postfix reload
```

لزيادة مقدار المعلومات المسجلة عند استكشاف مشاكل SASL، يمكنك ضبط الخيارات الآتية في ملف /etc/dovecot/conf.d/10-logging.conf:

```
auth_debug=yes
auth_debug_passwords=yes
```

ملاحظة: مثل Postfix، إذا عدّلت ضبط Dovecot فيجب إعادة تحميل العملية:

```
sudo service dovecot reload
```

ملاحظة: يمكن أن تزيد بعض الخيارات من مقدار المعلومات المُرسَلة إلى السجل زيادةً كبيرةً؛ تذكر أن تُعيد مستوى التسجيل إلى الحالة الطبيعية بعد أن تحلّ المشكلة؛ ثم أعد تحميل العفريت الملائم كي يأخذ الضبط الجديد مفعوله.

ح. مصادر

- يمكن أن تكون مهمة إدارة خادوم Postfix مهمةً معقدةً جدًا؛ وستحتاج في مرحلةٍ ما إلى الاستعانة بمجتمع أوبنتو للحصول على المساعدة.
- مكان رائع للسؤال عن مساعدة في Postfix والاشتراك في مجتمع أوبنتو هو قناة #ubuntu-server على خادوم freenode؛ يمكنك أيضًا نشر موضوع في أحد المنتديات.
- لمعلومات معمقّة عن Postfix، فينصح مطورو أوبنتو بكتاب «The Book of Postfix».
- موقع Postfix فيه توثيق رائع لمختلف خيارات الضبط المتوفرة.
- راجع أيضًا صفحة ويكي أوبنتو «Postfix» للمزيد من المعلومات.

٢. خادوم Exim4

إن Exim4 هو عميل نقل رسائل آخر مطور في جامعة كامبردج لاستخدامه في أنظمة يونكس المتصلة إلى الإنترنت؛ يمكن تثبيت Exim بدلًا من sendmail، وذلك على الرغم من أن ضبط exim مختلف كثيرًا عن ضبط sendmail.

ا. التثبيت

نفِّذ الأمر الآتي في الطرفية لتثبيت exim4:

```
sudo apt-get install exim4
```

ب. الضبط

نفِّذ الأمر الآتي لضبط Exim4:

```
sudo dpkg-reconfigure exim4-config
```

ستظهر واجهة مستخدم تسمح لك بضبط العديد من المعاملات؛ فمثلًا تُقسَّم ملفات الضبط في Exim4 إلى عدّة ملفات، إذا أردت أن تجعلهم في ملف واحد، فتستطيع ضبط ذلك من هذه الواجهة.

جميع المعاملات التي ضبطتها في واجهة المستخدم مخزنةٌ في الملف التالي /etc/exim4/update-exim4.conf؛ وإذا أردت إعادة الضبط، فتستطيع تشغيل معالج الضبط أو تعديل هذا الملف يدويًا باستخدام محررك النصي المفضل.

بعد أن تنتهي من الضبط، يمكنك تنفيذ الأمر الآتي لتولد ملف ضبط رئيسي:

```
sudo update-exim4.conf
```

يولَّد ويُخزَّن ملف الضبط الرئيسي في /var/lib/exim4/config.autogenerated.

تحذير: عليك عدم تعديل ملف الضبط الرئيسي /var/lib/exim4/config.autogenerated بتاتًا؛ حيث يُحدَّث تلقائيًا في كل مرة تُنفِّذ فيها update-exim4.conf.

نفِّذ الأمر الآتي لتشغيل عفريت Exim4:

```
sudo service exim4 start
```

ج. استيثاق SMTP

يشرح هذا القسم كيفية ضبط Exim4 لاستخدام SMTP-AUTH مع TLS و SASL.

أول خطوة هي إنشاء شهادة لاستخدامها مع TLS؛ وذلك بإدخال الأمر الآتي في الطرفية:

```
sudo /usr/share/doc/exim4-base/examples/exim-gencert
```

يجب أن يُضبَط Exim4 الآن لاستخدام TLS بتعديل الملف /etc/exim4/conf.d/main/03_exim4-config_tlsoptions وإضافة ما يلي:

```
MAIN_TLS_ENABLE = yes
```

ثـم سـتحتاج إلـى ضـبط Exim4 لاسـتخدام saslauthd للاسـتيثاق؛ عـدِّل الملـف /etc/exim4/conf.d/auth/30_exim4-config_examples وأزل التعليقـات عـن قسـمَيّ plain_saslauthd_server و login_saslauthd_server:

```
  plain_saslauthd_server:
    driver = plaintext
    public_name = PLAIN
    server_condition = ${if saslauthd{{$auth2}{$auth3}}{1}{0}}
    server_set_id = $auth2
    server_prompts = :
    .ifndef AUTH_SERVER_ALLOW_NOTLS_PASSWORDS
    server_advertise_condition = ${if eq{$tls_cipher}{}{}{*}}
    .endif
#
  login_saslauthd_server:
    driver = plaintext
    public_name = LOGIN
    server_prompts = "Username:: : Password::"
    # don't send system passwords over unencrypted connections
    server_condition = ${if saslauthd{{$auth1}{$auth2}}{1}{0}}
    server_set_id = $auth1
    .ifndef AUTH_SERVER_ALLOW_NOTLS_PASSWORDS
    server_advertise_condition = ${if eq{$tls_cipher}{}{}{*}}
    .endif
```

لكي يتمكن عميل البريد الخارجي من الاتصال إلى خادوم exim الجديد، فمن الضروري إضافة مستخدمين جدد إلى exim بتنفيذ الأوامر الآتية:

```
sudo /usr/share/doc/exim4/examples/exim-adduser
```

يجب أن يحمي المستخدمون ملفات كلمة المرور الجديدة لخادوم exim بالأوامر الآتية:

```
sudo chown root:Debian-exim /etc/exim4/passwd
sudo chmod 640 /etc/exim4/passwd
```

في النهاية، حدِّث ضبط Exim4 وأعد تشغيل الخدمة:

```
sudo update-exim4.conf
sudo service exim4 restart
```

د. ضبط SASL

يوفر هذا القسم معلومات حول ضبط خدمة saslauthd لتوفير الاستيثاق لخادوم Exim4.

أول خطوة هي تثبيت حزمة sasl2-bin من الطرفية بإدخال الأمر الآتي:

```
sudo apt-get install sasl2-bin
```

لضبط saslauthd، عدِّل ملف الضبط /etc/default/saslauthd واضبط START=no إلى:

```
START=yes
```

ثم يجب أن يكون المستخدم Debian-exim جزءًا من مجموعة sasl لكي يستخدم Exim4 الخدمةَ saslauthd:

```
sudo adduser Debian-exim sasl
```

عليك الآن تشغيل خدمة saslauthd:

```
sudo service saslauthd start
```

ضُبِط الآن Exim4 مع SMTP-AUTH ليستخدم TLS واستيثاق SASL.

٥. مصادر

- راجع موقع exim.org لمزيدٍ من المعلومات.
- يتوفر أيضًا كتاب «Exim4 Book».
- مصدر آخر هو صفحة ويكي أوبنتو «Exim4».

٣. برمجية Dovecot

إن Dovecot هو عميل تسليم البريد، مكتوبٌ مع اعتبار الحماية من الأولويات؛ ويدعم صيغتي صندوق البريد الرئيسيتين: mbox أو Maildir؛ يشرح هذا القسم كيفية ضبطه كخادوم imap أو pop3.

ا. التثبيت

نفِّذ الأمر الآتي في الطرفية لتثبيت dovecot:

```
sudo apt-get install dovecot-imapd dovecot-pop3d
```

ب. الضبط

عدِّل الملف /etc/dovecot/dovecot.conf لضبط dovecot، يمكنك اختيار البروتوكول الذي تريد استخدامه، حيث يمكن أن يكون pop3 أو pop3s (أي pop3 الآمن)، أو imap، أو imaps (أي imap الآمن)؛ شرح عن هذه البروتوكولات خارج عن نطاق هذا الكتاب، للمزيد من المعلومات راجع مقالات ويكيبيديا عنهم.

بروتوكولَي IMAPS و POP3S أكثر أمانًا من بروتوكولَي IMAP و POP3 لأنهما يستخدمان تشفير SSL للاتصال؛ بعد أن تختار البروتوكول، فعليك تعديل السطر الآتي في الملف /etc/dovecot/dovecot.conf:

```
protocols = pop3 pop3s imap imaps
```

ثم اختر صندوق البريد الذي تريد استخدامه، حيث يدعم Dovecot الصيغتين maildir و mbox؛ هاتان هما أشهر صيغتين مستعملتين للبريد؛ يملك كلاهما مزايا خاصةً به، ومشروحةً في موقع Dovecot.

بعد أن تختار نوع صندوق البريد، عدِّل الملف /etc/dovecot/conf.d/10-mail.conf وغيِّر السطر الآتي:

```
mail_location = maildir:~/Maildir # (for maildir)
```

أو

```
mail_location = mbox:~/mail:INBOX=/var/spool/mail/%u # (for
mbox)
```

ملاحظة: يجب عليك ضبط عميل نقل البريد (MTA) لنقل البريد الوارد إلى هذا النوع من صندوق البريد إذا كان مختلفًا عمّا ضبطته.

بعد الانتهاء من ضبط dovecot، يجب عليك إعادة تشغيل عفريت dovecot لتجرِّب عمل الخادوم:

```
sudo service dovecot restart
```

إذا فعّلت imap، أو pop3؛ فيجب عليك أيضًا تجربة تسجيل الدخول باستخدام الأوامر telnet localhost pop3 أو telnet localhost imap2؛ لترى إن شاهدت شيئًا شبيهًا بما يلي، فستعلم أن التثبيت والإعداد قد نجحا:

```
user@localbox:~$ telnet localhost pop3
Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^]'.
+OK Dovecot ready.
```

ج. ضبط Dovecot SSL

لضبط Dovecot ليستخدم SSL، حرّر الملف /etc/dovecot/conf.d/10-ssl.conf وعدّل الأسطر الآتية:

```
ssl = yes
ssl_cert = </etc/ssl/certs/dovecot.pem
ssl_key = </etc/ssl/private/dovecot.pem
```

يمكنك الحصول على شهادة SSL من سلطة إصدار الشهادات أو إنشاء شهادة SSL موقعة ذاتيًا؛ الخيار الأخير هو خيار جيد للبريد الإلكتروني، لأن عملاء SMTP نادرًا ما يشتكون حول الشهادات الموقعة ذاتيًا؛ رجاءً عُد إلى الفصل التاسع لمزيد من المعلومات حول إنشاء شهادة SSL موقعة ذاتيًا؛ يجب عليك الحصول على ملف مفتاح وملف الشهادة بعد إنشائك للشهادة؛ رجاءً انسخهما إلى المكان المُشار إليه في ملف الضبط /etc/dovecot/conf.d/10-ssl.conf.

د. ضبط الجدار الناري لخادوم البريد الإلكتروني

عليك ضبط الجدار الناري للسماح للاتصالات على المنافذ الضرورية للوصول إلى خادوم البريد من حاسوبٍ آخر، وهي:

```
IMAP - 143
IMAPs - 993
POP3 - 110
POP3s - 995
```

ه. مصادر

- راجع موقع Dovecot لمزيدٍ من المعلومات.
- أيضًا صفحة ويكي أوبنتو «Dovecot» فيها تفاصيلٌ إضافية.

٤. برمجية Mailman

إن Mailman هـو برمجيـة مفتوحـة المصـدر لإدارة نقاشـات البريـد الإلكـتروني وقـوائم الأخبـار الإلكترونيـة؛ وتعتمـد العديـد مـن قـوائم البريـد المفتوحـة المصـدر (بمـا فيهـا قـوائم بريـد أوبنتو) على Mailman كبرمجية قوائم البريد؛ حيث أنها قوية وسهلة التثبيت والإدارة.

ا. التثبيت

يـوفر Mailman واجهـة ويـب للمـدراء والمسـتخدمين؛ مسـتخدمًا خـادوم بريـد خـارجي لإرسال واستقبال الرسائل؛ حيث يعمل عملًا ممتازًا مع خواديم البريد الآتية:

- Postfix
- Exim
- Sendmail
- Qmail

سنتعلم طريقة تثبيت وضبط Mailman مع خادوم ويب أباتشي ومع أحد خادومَي البريد Postfix أو Exim؛ إذا أردت استخدام Mailman مع خادوم بريد مختلف، فرجاءً عُد إلى قسم المصادر لمزيدٍ من المعلومات.

ملاحظة: تحتاج إلى خادوم بريد وحيد فقط، و Postfix هو عميل نقل البريد الافتراضي في أوبنتو.

Apache2

لتثبيت apache2، راجع الفصل الحادي عشر لمزيد من التفاصيل.

Postfix

راجع القسم الأول من هذا الفصل لتعليمات عن تثبيت وضبط Postfix.

Exim4

لتثبيت Exim4، راجع القسم الثاني من هذا الفصل.

تُخزَّن ملفات الضبط في مجلد /etc/exim4 بعد تثبيت exim4؛ وتكون ملفات ضبط exim4 مقسمة إلى عدة ملفات مختلفة افتراضيًا في أوبنتو؛ يمكنك تغيير هذا السلوك بتعديل قيمة المتغير الآتي في ملف /etc/exim4/update-exim4.conf:

```
dc_use_split_config='true'
```

Mailman

نفِّذ الأمر الآتي في الطرفية لتثبيت Mailman:

```
sudo apt-get install mailman
```

تنسخ هذه الحزمة ملفات التثبيت إلى مجلد /var/lib/mailman، وتثبت سكربتات CGI في /usr/lib/cgi-bin/mailman؛ وستُنشِئ مستخدم لينُكس المسمى list، وكذلك تُنشِئ المجموعة list؛ ستُملَك عملية mailman لهذا المستخدم.

ب. الضبط

يفترض هذا القسم أنك ثبتت mailman و apache2 و postfix أو exim4 بنجاح؛ كل ما بقي عليك هو ضبطهم.

مثالٌ عن ملف ضبط أباتشي يأتي مع Mailman الموجود في /etc/mailman/apache.conf، ولكي يستخدم أباتشي ملف الضبط هذا، فيجب أن يُنسَخ إلى /etc/apache2/sites-available:

```
sudo cp /etc/mailman/apache.conf \
/etc/apache2/sites-available/mailman.conf
```

هذا سيُنشِئ مضيفًا وهميًا في أباتشي لموقع إدارة Mailman؛ فعِّل الآن الضبط الجديد وأعد تشغيل أباتشي:

```
sudo a2ensite mailman.conf
sudo service apache2 restart
```

يستخدم Mailman أباتشي ليشغِّل سكربتات CGI؛ تكون سكربتات CGI مثبتةً في /usr/lib/cgi-bin/mailman، هذا يعني أن وصلة mailman ستكون على الرابط التالي http://hostname/cgi-bin/mailman؛ يمكنك إجراء تعديلات على الملف التالي /etc/apache2/sites-available/mailman.conf لتعديل هذا السلوك.

Postfix

سنربط النطاق lists.example.com مع القائمة البريدية للدمج مع Postfix؛ رجاءً استبدل lists.example.com بالنطاق الذي تختاره.

يمكنك استخدام الأمر postconf لإضافة الضبط الضروري إلى ملف /etc/postfix/main.cf:

```
sudo postconf -e 'relay_domains = lists.example.com'
sudo postconf -e 'transport_maps = hash:/etc/postfix/transport'
sudo postconf -e 'mailman_destination_recipient_limit = 1'
```

انظر أيضًا في /etc/postfix/master.cf للتحقق من أن لديك «الناقل» (transporter) الآتي:

```
mailman    unix    -    n    n    -    -    pipe
  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-
mailman.py ${nexthop} ${user}
```

هذا سيستدعي السكربت postfix-to-mailman.py عندما يُسلَّم بريدٌ ما إلى القائمة.

اربط بين النطاق lists.example.com إلى ناقل Mailman باستخدام خريطة الربط (transport map)، وعدِّل الملف /etc/postfix/transport:

```
lists.example.com      mailman:
```

عليك الآن جعل Postfix يبني خريطة الربط بإدخال الأمر الآتي في الطرفية:

```
sudo postmap -v /etc/postfix/transport
```

ثم أعد تشغيل Postfix لتفعيل الضبط الجديد:

```
sudo service postfix restart
```

Exim4

تستطيع تشغيل خادوم Exim بإدخال الأمر الآتي في الطرفية بعد تثبيت Exim4:

```
sudo service exim4 start
```

ولجعل mailman يعمل مع Exim4، فيجب عليك أن تضبط Exim4؛ وكما ذُكِرَ سابقًا، يستخدم Exim4 افتراضيًا عدّة ملفات ضبط للأنواع المختلفة؛ لمزيد من التفاصيل، ارجع إلى موقع ويب Exim. يجب عليك إضافة ملف ضبط جديد يحتوي على أنواع الضبط الآتية لتشغيل mailman:

١. Main (الرئيسي).

٢. Transport (النقل).

٣. Router (الموجه).

يُنشِئ Exim ملف ضبط رئيسي بترتيب كل ملفات الضبط الصغيرة هذه؛ ولذلك ترتيب هذه الملفات أمرٌ ضروريٌ جدًا.

الرئيسي

جميع ملفات الضبط التي تنتمي إلى النوع الرئيسي (Main) يجب أن تُخزَّن في مجلد /etc/exim4/conf.d/main/، يمكنك إضافة المحتويات الآتية في ملف جديد مُسمى 04_exim4-config_mailman:

```
# start
# Home dir for your Mailman installation -- aka Mailman's
prefix
# directory.
# On Ubuntu this should be "/var/lib/mailman"
# This is normally the same as ~mailman
MM_HOME=/var/lib/mailman
#
# User and group for Mailman, should match your --with-mail-gid
# switch to Mailman's configure script.            Value is
normally "mailman"
MM_UID=list
MM_GID=list
#
# Domains that your lists are in - colon separated list
# you may wish to add these into local_domains as well
domainlist mm_domains=hostname.com
#
# -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
#
# These values are derived from the ones above and should not
need
# editing unless you have munged your mailman installation
#
# The path of the Mailman mail wrapper script
MM_WRAP=MM_HOME/mail/mailman
#
# The path of the list config file (used as a required file
when
# verifying list addresses)
MM_LISTCHK=MM_HOME/lists/${lc::$local_part}/config.pck
# end
```

النقل

جميع الملفات التي تنتمي إلى نوع النقل (transport) يجب أن تُخزَّن في مجلد /etc/exim4/conf.d/transport/؛ تستطيع إضافة المحتويات الآتية إلى ملف جديد باسم 40_exim4-config_mailman:

```
mailman_transport:
 driver = pipe
 command = MM_WRAP \
              '${if def:local_part_suffix \
                      {${sg{$local_part_suffix}{-(\\w+)(\\
+.*)?}{\$1}}} \
                      {post}}' \
              $local_part
  current_directory = MM_HOME
  home_directory = MM_HOME
  user = MM_UID
  group = MM_GID
```

الموجه

جميع الملفات التي تنتمي إلى نوع الموجه (router) يجب أن تُخزَّن في مجلد /etc/exim4/conf.d/router/؛ تستطيع إضافة المحتويات الآتية إلى ملف جديد باسم 101_exim4-config_mailman:

```
  mailman_router:
    driver = accept
    require_files = MM_HOME/lists/$local_part/config.pck
    local_part_suffix_optional
    local_part_suffix = -bounces : -bounces+* : \
                            -confirm+* : -join : -leave : \
                            -owner : -request : -admin
    transport = mailman_transport
```

تحذير: ترتيب ملفات الضبط «الرئيسي» و«النقل» غير مهم، لكن ترتيب ملفات ضبط التوجيه مهم؛ حيث يجب أن يظهر هذا الملف قبل ملف 200_exim4-config_primary؛ هذان الملفان يحتويان على نفس نوع المعلومات، وتكون الأولوية للذي يأتي أولًا.

Mailman

بعد تثبيت mailman، تستطيع تشغيله بالأمر الآتي:

```
sudo service mailman start
```

عليك الآن إنشاء قائمة بريدية افتراضية؛ وذلك بتنفيذ ما يلي:

```
sudo /usr/sbin/newlist mailman

  Enter the email address of the person running the list: user
at ubuntu.com
  Initial mailman password:
  To finish creating your mailing list, you must edit your
/etc/aliases (or
  equivalent) file by adding the following lines, and possibly
running the
  `newaliases' program:

  ## mailman mailing list
  mailman:              "|/var/lib/mailman/mail/mailman
post mailman"
  mailman-admin:        "|/var/lib/mailman/mail/mailman
admin mailman"
  mailman-bounces:      "|/var/lib/mailman/mail/mailman
bounces mailman"
  mailman-confirm:      "|/var/lib/mailman/mail/mailman
confirm mailman"
  mailman-join:         "|/var/lib/mailman/mail/mailman
join mailman"
  mailman-leave:        "|/var/lib/mailman/mail/mailman
leave mailman"
```

```
  mailman-owner:              "|/var/lib/mailman/mail/mailman
owner mailman"
  mailman-request:            "|/var/lib/mailman/mail/mailman
request mailman"
  mailman-subscribe:          "|/var/lib/mailman/mail/mailman
subscribe mailman"
  mailman-unsubscribe:        "|/var/lib/mailman/mail/mailman
unsubscribe mailman"

  Hit enter to notify mailman owner...

  #
```

لقد ضبطنا إما Postfix أو Exim4 للتعرف على كل البريد من mailman؛ لذلك ليس ضروريًا إنشاء أيّة قيود جديدة في /etc/aliases؛ إذا أجريت أيّة تعديلات إلى ملفات الضبط، فرجاءً تأكد أنك أعدت تشغيل هذه الخدمات قبل الإكمال إلى القسم الآتي.

ملاحظة: لا يَستخدِم Exim4 الأسماء البديلة في الأعلى لتمرير البريد إلى Mailman، حيث أنه يستخدم طريقة «الاكتشاف»؛ لتجاهل الأسماء البديلة (aliases) عند إنشاء القائمة، فأضف السطر MTA=None إلى ملف ضبط Mailman، الذي هو /etc/mailman/mm_cfg.py.

ج. الإدارة

لنفرض أن لديك تثبيتًا افتراضيًا وأنّك أبقيت على سكربتات CGI في المجلد التالي /usr/lib/cgi-bin/mailman/. يوفر Mailman أداة ويب للإدارة؛ وجّه متصفحك إلى العنوان الآتي للوصول إليها:

```
http://hostname/cgi-bin/mailman/admin
```

ستظهر القائمة البريدية الافتراضية على الشاشة وهي mailman؛ إذا ضغطت على اسم القائمة البريدية، فستُسأل عن كلمة المرور للاستيثاق؛ إذا أدخلت كلمة مرور صحيحة، فستكون قادرًا على تغيير الإعدادات الإدارة للقائمة البريدية؛ يمكنك إنشاء قائمة بريدية جديدة باستخدام الأداة السطرية /usr/sbin/newlist؛ أو بشكل بديل يمكنك إنشاؤها عبر واجهة الويب.

د. المستخدمون

يوفر Mailman واجهة ويب للمستخدمين، وجِّه متصفحك نحو العنوان الآتي للوصول لتلك الصفحة:

```
http://hostname/cgi-bin/mailman/listinfo
```

ستظهر القائمة البريدية الافتراضية mailman على الشاشة؛ وإذا ضغطت على اسم القائمة البريدية، فسيظهر نموذج للاشتراك فيها؛ يمكنك إدخال بريدك الإلكتروني واسمك (اختياري) وكلمة المرور للاشتراك؛ سيُرسَل بريد للدعوة إلى بريدك الإلكتروني، ويمكنك اتباع التعليمات في البريد للاشتراك.

ه. مصادر

- دليل تثبيت GNU Mainman.
- HOWTO – Using Exim 4 and Mailman 2.1 together.
- راجع أيضًا صفحة ويكي أوبنتو «Mailman».

٥. ترشيح البريد

واحدة من أكبر المشاكل مع البريد الإلكتروني اليوم هي مشكلة البريد غير المرغوب فيه (Unsolicited Bulk Email أو اختصارًا UBE) المعروف أيضًا بالبريد العشوائي (SPAM)؛ قد تحتوي هذه الرسائل أيضًا على فيروسات أو أشكالٍ أخرى من البرمجيات الخبيثة؛ ووفقًا لبعض التقارير، تشغل هذه الرسائل حيزًا كبيرًا من البريد الإلكتروني المُرسَل عبر الإنترنت.

سيشرح هذا القسم طريقة دمج Amavisd-new، و Spamassassin، و ClamAV مع عميل نقل البريد Postfix؛ يمكن أيضًا التحقق من البريد عبر تمريره خلال مرشحات خارجية؛ هذه المرشحات يمكنها في بعض الأحيان تحديد إذا ما كانت الرسالةُ عشوائيةً دون الحاجة إلى معالجتها ببرمجيات تستهلك الموارد؛ أشهر هذه المرشحات هي opendkim و python-policyd-spf.

- إن Amavisd-new هو برنامج مُغلِّف (wrapper) يستطيع استدعاء أي عدد من برامج ترشيح المحتوى لاستكشاف الرسائل العشوائية، وللتصدي للفيروسات ...إلخ.
- يستخدم Spamassassin آلياتٍ عدّة لترشيح البريد اعتمادًا على محتوى الرسالة.
- إن ClamAV هو مضاد فيروسات مفتوح المصدر.
- يوفر opendkim ما يسمى Milter (أي Sendmail Mail Filter) إلى المعيار القياسي DKIM (أي DomainKeys Identified Mail).
- يُفعِّل python-policyd-spf تحقق SPF (اختصار للعبارة Sender Policy Framework) مع Postfix.

هذه هي آلية جمع القطع السابقة:

- تُقبَل رسالة البريد الإلكتروني من Postfix.
- تُمرَّر الرسالة إلى أي مرشحات خارجية مثل opendkim و python-policyd-spf في هذه الحالة.
- ثم يُعالِج Amavisd-new الرسالة.
- ثم يُستخدَم ClamAV لفحص الرسالة؛ إذا حوت الرسالة على فيروس، فسيرفضها Postfix.
- ستُحلَّل الرسائل «النظيفة» من Spamassassin للتحقق إذا كانت الرسالة هي رسالة عشوائية؛ ثم يضيف Spamassassin أسطر X-Header ليسمح للبرمجية Amavisd-new بإكمال معالجة الرسالة.

على سبيل المثال، إذا كان «رصيد العشوائية» لرسالة ما أكبر من خمسين بالمئة، فيمكن أن تُزال الرسالة تلقائيًا من الطابور (queue) حتى دون إعلام المتلقي؛ طريقة أخرى للتعامل مع هذه الرسائل هي إيصالهم لعميل مستخدم البريد (MUA) والسماح للمستخدم بأن يتعامل مع الرسالة بما يراه مناسبًا.

ا. التثبيت

راجع القسم الأول من هذا الفصل لمعلوماتٍ تفصيلية عن تثبيت Postfix.

أدخل الأمرين الآتيين في سطر الأوامر لتثبيت بقية البرمجيات:

```
sudo apt-get install amavisd-new spamassassin clamav-daemon
sudo apt-get install opendkim postfix-policyd-spf-python
```

هنالك بعض الحزم الأخرى التي يمكن أن تُدمَج مع Spamassassin لاكتشاف أفضل للرسائل العشوائية:

```
sudo apt-get install pyzor razor
```

بالإضافة إلى برمجيات الترشيح الرئيسية، سنحتاج إلى أدوات الضغط لنعالج بعض مرفقات البريد:

```
sudo apt-get install arj cabextract cpio lha nomarch pax rar
unrar unzip zip
```

ملاحظة: إذا لم يُعثَر على بعض الحزم السابقة، فتأكد من تفعيل مستودع multiverse في الملف التالي /etc/apt/sources.list.

إذا أجريتَ تعديلاتٍ على ذاك الملف، فتأكد من تحديث فهرس الحزم بتنفيذ الأمر sudo apt-get update قبل محاولة التثبيت مرةً أخرى.

ب. الضبط

علينا الآن ضبط كل شيء مع بعضه بعضًا لترشيح البريد.

ClamAV

السلوك الافتراضي لبرمجية ClamAV تناسب احتياجاتنا؛ للمزيد من خيارات الضبط الخاصة ببرمجية ClamAV، راجع ملفات الضبط في /etc/clamav.

أضف المستخدم clamav إلى المجموعة amavis لكي يملك Amavisd-new الوصول الملائم لتفحص الملفات:

```
sudo adduser clamav amavis
sudo adduser amavis clamav
Spamassassin
```

يعثر Spamassassin تلقائيًا على المكونات الإضافية ويستخدمها إن توفرت؛ هذا يعني أنه لا حاجة لضبط pyzor و razor.

عدِّل ملف الضبط /etc/default/spamassassin لتفعيل عفريت Spamassassin، عدِّل قيمة ENABLED=0 إلى:

```
ENABLED=1
```

ثم ابدأ تشغيل العفريت:

```
sudo service spamassassin start
```

Amavisd-new

أولًا، فعّل استكشاف الرسائل العشوائية ومضاد الفيروسات في Amavisd-new بتعديل الملف /etc/amavis/conf.d/15-content_filter_mode:

```
use strict;

# You can modify this file to re-enable SPAM checking through
spamassassin
# and to re-enable antivirus checking.

#
# Default antivirus checking mode
# Uncomment the two lines below to enable it
#

@bypass_virus_checks_maps = (
    \%bypass_virus_checks, \@bypass_virus_checks_acl, \
$bypass_virus_checks_re);

#
# Default SPAM checking mode
# Uncomment the two lines below to enable it
#

@bypass_spam_checks_maps = (
    \%bypass_spam_checks, \@bypass_spam_checks_acl, \
$bypass_spam_checks_re);

1;    # insure a defined return
```

قد تكون إعادة معالجة الرسائل العشوائية فكرةً سيئةً لأن العنوان المُعاد مزيفٌ غالبًا؛ ربما ترغب بتعديل الملف /etc/amavis/conf.d/20-debian_defaults لتضبط $final_spam_destiny إلى D_DISCARD بدلًا من D_BOUNCE، كما يلي:

```
$final_spam_destiny       = D_DISCARD;
```

وربما ترغب بتعديل قيمة الخيارات الآتية لتعليم (flag) المزيد من الرسائل كرسائل عشوائية:

```
$sa_tag_level_deflt = -999; # add spam info headers if at, or
above that level
$sa_tag2_level_deflt = 6.0; # add 'spam detected' headers at
that level
$sa_kill_level_deflt = 21.0; # triggers spam evasive actions
$sa_dsn_cutoff_level = 4; # spam level beyond which a DSN is
not sent
```

إذا كان اسم المضيف للخادوم (hostname) مختلفًا عن سجل MX للنطاق، فربما تحتاج إلى أن تضبط الخيار $myhostname يدويًا؛ وإذا كان الخادوم يستلم البريد لأكثر من نطاق، فيجب تخصيص الخيار @local_domains_acl أيضًا، وذلك بتعديل الملف /etc/amavis/conf.d/50-user:

```
$myhostname = 'mail.example.com';
@local_domains_acl = ( "example.com", "example.org" );
```

إذا أردت تغطية أكثر من نطاق، فعليك استخدام ما يلي في /etc/amavis/conf.d/50-user:

```
@local_domains_acl = qw(.);
```

يجب إعادة تشغيل Amavisd-new بعد الضبط:

```
sudo service amavis restart
```

٦. قائمة DKIM البيضاء

يمكن ضبط Amavisd-new ليضيف عناوين من نطاقات معينة مع مفاتيح نطاق (Domain Keys) صالحة إلى القائمة البيضاء (Whitelist)؛ هنالك بعض النطاقات المضبوطة مسبقًا في /etc/amavis/conf.d/40-policy_banks:

هذه بعض الأمثلة لضبط القائمة البيضاء لنطاق:

- التعليمة 'example.com' => 'WHITELIST',: ستضيف أي عنوان من النطاق "example.com" إلى القائمة البيضاء.
- التعليمة '.example.com' => 'WHITELIST',: ستضيف أي عنوان من أي نطاق فرعي للنطاق "example.com" ويملك توقيع صالح (valid signature) إلى القائمة البيضاء.
- التعليمة '.example.com/@example.com' => 'WHITELIST',: إضافة أي عنوان من النطاقات الفرعية للنطاق "example.com" الذي يستخدم توقيع النطاق الأب "example.com".
- التعليمة './@example.com' => 'WHITELIST',: يضيف العناوين من توقيع صالح من "example.com" هذا يستخدم عادةً لمجوعات النقاش التي توقِّع رسائلها.

يمكن أن يملك نطاقٌ واحد أكثر من ضبط للقائمة البيضاء؛ عليك إعادة تشغيل amavisd-new بعد تعديل الملف:

```
sudo service amavis restart
```

ملاحظة: في هذا السياق؛ عندما يُضاف النطاق إلى القائمة البيضاء، فإن الرسالة لن تحصل على أي فحص من الفيروسات أو الرسائل العشوائية؛ ربما يكون أو لا يكون هذا هو السلوك الذي ترغبه لهذا النطاق.

ا. في Postfix

أدخل ما يلي في مِحَث الطرفية لدمج Postfix:

```
sudo postconf -e 'content_filter = smtp-amavis: \
[127.0.0.1]:10024'
```

ثم عدِّل الملف /etc/postfix/master.cf وأضف الأسطر الآتية إلى نهاية الملف:

```
smtp-amavis     unix    -       -       -       -       2     smtp
     -o smtp_data_done_timeout=1200
     -o smtp_send_xforward_command=yes
     -o disable_dns_lookups=yes
     -o max_use=20
127.0.0.1:10025 inet    n       -       -       -       -     smtpd
     -o content_filter=
     -o local_recipient_maps=
     -o relay_recipient_maps=
     -o smtpd_restriction_classes=
     -o smtpd_delay_reject=no
     -o smtpd_client_restrictions=permit_mynetworks,reject
     -o smtpd_helo_restrictions=
     -o smtpd_sender_restrictions=
     -o smtpd_recipient_restrictions=permit_mynetworks,reject
     -o smtpd_data_restrictions=reject_unauth_pipelining
     -o smtpd_end_of_data_restrictions=
     -o mynetworks=127.0.0.0/8
     -o smtpd_error_sleep_time=0
     -o smtpd_soft_error_limit=1001
     -o smtpd_hard_error_limit=1000
     -o smtpd_client_connection_count_limit=0
     -o smtpd_client_connection_rate_limit=0
     -o
receive_override_options=no_header_body_checks,no_unknown_recip
ient_checks
```

أيضًا أضف السطرين الآتيين مباشرةً بعد خدمة النقل «pickup»:

```
    -o content_filter=
    -o receive_override_options=no_header_body_checks
```

هذا سيمنع الرسائل المُولّدة للتبليغ عن الرسائل العشوائية من تصنيفها كرسائل عشوائية؛

أعد الآن تشغيل Postfix:

```
sudo service postfix restart
```

يجب الآن أن يكون ترشيح المحتوى والعثور على الفيروسات مُفعَّلًا.

ب. الاختبار

أولًا، اختبر أن Amavisd-new SMTP يستمع:

```
telnet localhost 10024
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 [127.0.0.1] ESMTP amavisd-new service ready
^]
```

وفي ترويسة (header) الرسائل التي تُمرَّر عبر مُرشِّح المحتوى، يجب أن تُشاهِد:

```
X-Spam-Level:
X-Virus-Scanned: Debian amavisd-new at example.com
X-Spam-Status: No, hits=-2.3 tagged_above=-1000.0 required=5.0
tests=AWL, BAYES_00
X-Spam-Level:
```

ملاحظة: قد تختلف النتائج المعروضة عمًا سيظهر عندك، لكن من المهم وجود القيدين X-Virus-Scanned و X-Spam-Status.

ج. استكشاف الأخطاء

أفضل طريقة لمعرفة سبب حدوث مشكلة ما هي مراجعة ملفات السجل. لتعليماتٍ عن التسجيل في Postfix راجع القسم الأول من هذا الفصل.

يستخدم Amavisd-new البرمجية Syslog لإرسال الرسائل إلى /var/log/mail.log؛ يمكن زيادة مقدار التفاصيل بإضافة الخيار $log_level إلى ملف /etc/amavis/conf.d/50-user، وضبط القيمة من ١ إلى ٥:

```
$log_level = 2;
```

ملاحظة: عند زيادة درجة الإسهاب لسجل Amavisd-new، فسيزداد ناتج سجل Spamassassin أيضًا.

يمكن زيادة مستوى التسجيل لبرمجية ClamAV بتعديل الملف /etc/clamav/clamd.conf وضبط الخيار الآتي:

```
LogVerbose true
```

افتراضيًا، سيُرسِل ClamAV رسائل السجل إلى /var/log/clamav/clamav.log.

ملاحظة: بعد تغيير إعدادات التسجيل للبرمجيات، تذكر أن تعيد تشغيل الخدمة لكي تأخذ الإعدادات الجديدة مفعولها؛ أيضًا تذكر أن تعيد القيمة الافتراضية بعد أن تحل المشكلة.

د. مصادر

للمزيد من المصادر حول ترشيح البريد، راجع الوصلات الآتية:

- توثيق Amavisd-new.
- توثيق ClamAV وويكي ClamAV.
- ويكي Spamassassin.
- صفحة Pyzor الرئيسية.
- صفحة Razor الرئيسية على سورس فورج.

موقع DKIM.org.

- Postfix Amavis New.
- أيضًا، تستطيع أن تسأل أسئلتك في قناة ubuntu-sever# على خادوم freenode.



تطبيقات المحادثة

سنناقش في هذا الفصل كيفية تثبيت وضبط خادوم IRC ‏(ircd-irc2) وسنناقش أيضًا كيفية تثبيت وضبط خادوم المراسلة الفورية Jabber.

ا. خادوم IRC

يحتوي مستودع أوبنتو على العديد من خواديم IRC، يشرح هذا القسم كيفية تثبيت وضبط خادوم IRC الأصلي ircd-irc2.

ا. التثبيت

أدخِل الأمر الآتي في الطرفية لتثبيت خادوم ircd-irc2:

```
sudo apt-get install ircd-irc2
```

يُخزَّن ملف الضبط في مجلد /etc/ircd، والتوثيق متوفرٌ في المجلد في المسار التالي: /usr/share/doc/ircd-irc2.

ب. الضبط

يمكن أن تُضبَط إعدادات IRC بملف الضبط /etc/ircd/ircd.conf؛ يمكنك ضبط اسم مضيف IRC بتعديل السطر الآتي:

```
M:irc.localhost::Debian ircd default configuration::000A
```

رجاءً تأكد أنك تضيف أسماء DNS البديلة لاسم مضيف IRC؛ على سبيل المثال، إذا ضبطت irc.liveciper.com كاسم مضيف IRC؛ فتأكد أن irc.liveciper.com يُحَّل في خادوم أسماء المضيفين عندك؛ لا يتوجب أن يكون اسم مضيف IRC هو نفسه اسم مضيف الخادوم.

يمكن ضبط معلومات مدير IRC بتعديل السطر الآتي:

```
A:Organization, IRC dept.:Daemon <ircd@example.irc.org>:Client
Server::IRCnet:
```

عليك إضافة أسطر خاصة لضبط قائمة بالمنافذ التي يستمع إليها IRC؛ ولضبط «الأوراق الاعتمادية للمشغل»، ولتضبط الاستيثاق من العميل ...إلخ. رجاءً ارجع إلى المثال عن ملف الضبط الموجود في ‎/usr/share/doc/ircd-irc2/ircd.conf.example.gz.

لافتة IRC هي الرسالة التي تظهر في عميل IRC عندما يتصل إلى الخادوم، ويمكن أن تُضبَط في الملف ‎/etc/ircd/ircd.motd.

بعد إجراء التعديلات الضرورية لملف الضبط، تستطيع إعادة تشغيل خادوم IRC بتنفيذ الأمر الآتي:

```
sudo service ircd-irc2 restart
```

ج. مصادر

- ربما تكون مهتمًا بإلقاء نظرة إلى خواديم IRC الأخرى المتوفرة في مستودعات أوبنتو، التي تتضمن ircd-ircu، و ircd-hybrid.
- ارجع إلى IRCD FAQ للمزيد من التفاصيل حول خادوم IRC.

٢. خادوم المراسلة الفورية Jabber

إن Jabber هـو بروتوكـول مراسـلة فوريـة مبنـي علـى XMPP (معيـار مفتـوح للمراسـلة الفوريـة) ويُسـتخدَم بواسـطة عـدّة برمجيـات مشـهورة. يشـرح هـذا القسـم طريقـة إعـداد خـادوم Jabberd 2 على شبكة LAN محلية؛ يمكن أن يُعدَّل هذا الضبط لتوفير خدمات تبادل الرسائل فوريًا عبر الإنترنت.

ا. التثبيت

لتثبيت jabberd2، أدخِل الأمر الآتي في الطرفية:

```
sudo apt-get install jabberd2
```

ب. الضبط

هنالـك ملفَـيّ ضبـط XML يُسـتخدَمان لضبـط Jabberd2 لاسـتيثاق Berkeley DB مـن المسـتخدم؛ هـذا شـكل بسـيط جـدًا مـن أشـكال الاسـتيثاق؛ لكـن يمكـن ضـبط Jabberd2 لكـي يَستخدم LDAP، أو MySQL، أو PostgreSQL ...إلخ. للاستيثاق من المستخدم.

أولًا، عدِّل الملف /etc/jabberd2/sm.xml مغيّرًا:

```
<id>jabber.example.com</id>
```

ملاحظة: استبدل jabber.example.com باسم المضيف أو بمعرِّف ID آخر لخادومك.

الآن في قسم <storage>، عدِّل قيمة <driver> إلى:

```
<driver>db</driver>
```

ثم في ملف /etc/jabberd2/c2s.xml، عدِّل في قسم <local>:

```
<id>jabber.example.com</id>
```

وعدِّل أيضًا <module> في قسم <authreg> إلى:

```
<module>db</module>
```

في النهاية، أعد تشغيل خدمة jabberd2 لتفعيل الضبط الجديد:

```
sudo service jabberd2 restart
```

يمكنك الآن الاتصال على الخادوم بعميل Jabber مثل بيدجن (Pidgin) على سبيل المثال.

ملاحظة: ميزة استخدام Berkeley DB لمعلومات المستخدم هو أنها لا تحتاج إلى صيانة إضافية بعد ضبطها؛ إذا أردت المزيد من التحكم في حسابات المستخدمين، فمن المستحسن استخدام آلية استيثاق أخرى.

ج. مصادر

- يحتوي موقع Jabberd2 على المزيد من التفاصيل حول ضبط Jabberd2.
- للمزيد من خيارات الاستيثاق، راجع «Jabberd2 Install Guide».
- أيضًا، هنالك بعض المعلومات في صفحة ويكي أوبنتو «Setting Up Jabber Server».

١٧

أنظمة التحكم بالإصدارات

التحكم بالإصدارات (Version Control) هو فن إدارة التغييرات إلى المعلومات؛ وهي أداة محورية للمبرمجين، الذين يستهلكون وقتهم بإجراء تعديلات صغيرة إلى البرمجيات ومن ثم يتراجعون عنها في اليوم التالي! لكن فائدة برمجيات التحكم بالإصدارات تمتد خارج حدود عالم تطوير البرمجيات؛ في أي مكان تجد فيه أشخاصًا يستخدمون الحواسيب لإدارة معلومات تتغير عادةً، فهنالك مكان للتحكم بالإصدارات.

ا. نظام Bazaar

إن Bazaar هو نظام جديد للتحكم بالإصدارات ممول من كانونيكال - الشركة التجارية التي تقف خلف أوبنتو، وعلى النقيض من Subversion و CVS اللذان يدعمان نمط المستودع المركزي، فإن Bazaar يدعم أيضًا «التحكم الموزَّع بالإصدارات» (distributed version control)، مما يسمح للناس بالتعامل بطريقة تعاونية أكثر فعاليةً؛ وخصوصًا أن Bazaar مصمم لتعظيم درجة اشتراك المجتمع في المشاريع المفتوحة المصدر.

ا. التثبيت

أدخِل الأمر الآتي في الطرفية لتثبيت bzr:

```
sudo apt-get install bzr
```

ب. الضبط

لكي «تُعرِّف نفسك» إلى bzr، فاستخدم الأمر whoami كما يلي:

```
bzr whoami 'Joe Doe <joe.doe@gmail.com>'
```

ج. تعلم Bazaar

يأتي Bazaar مع توثيق مدمج مثبَّت في /usr/share/doc/bzr/html افتراضيًا؛ يأتي الأمر bzr أيضًا مع مساعدة مدمجة فيه:

```
bzr help
```

لتعلم المزيد عن أمرٍ ما:

```
bzr help foo
```

د. الدمج مع Launchpad

على الرغم من أنه مفيد كنظام يعمل بمفرده، لكنه يملك قابلية الدمج الاختياري مع Launchpad، الذي هو نظام التطوير التعاوني المستخدم من كانونيكال ومجتمع البرمجيات المفتوحة المحيط بها لإدارة وتوسيع أوبنتو؛ للمزيد من المعلومات حول كيفية استخدام Bazaar مع Launchpad للتعاون في البرمجيات مفتوحة المصدر، راجع Launchpad Integration.

٢. نظام Git

إن Git هو نظام تحكم بالإصدارات موزَّع (distributed) ومفتوح المصدر مطوَّر من لينوس تورفالدس لدعم تطوير نواة لينُكس؛ حيث يكون كل مجلد في Git عبارة عن مستودع مع تأريخ كامل وإمكانيات لتتبع الإصدارات، وليس متعمِدًا على الوصول على الشبكة أو على خادوم مركزي.

ا. التثبيت

يمكن تثبيت نظام التحكم بالإصدارات git باستخدام الأمر الآتي:

```
sudo apt-get install git
```

ب. الضبط

يجب لكل مستخدم git أن يعرِّف نفسه أولًا إلى git، وذلك بتنفيذ الأمرّين الآتيين:

```
git config --global user.email "you@example.com"
git config --global user.name "Your Name"
```

ج. الاستخدام الأساسي

ما سبق يكفي لاستخدام git في طريقة موزعة وآمنة، حيث يُفترَض أنَّ المستخدمين يستطيعون الوصول إلى الخادوم عبر SSH؛ حيث يمكن إنشاء مستودع جديد على الخادوم بالأمر:

```
git init --bare /path/to/repository
```

ملاحظة: الأمر السابق يُنشِئ مستودعًا «فارغًا» (bare)، أي أنه ليس بالإمكان استخدامه للتعديل على الملفات مباشرةً. إذا أردت الحصول على نسخة من محتويات المستودع على الخادوم، فاحذف الخيار bare--.

يمكن لأي عميل يملك وصولًا عبر SSH إلى الخادوم أن ينسخ المستودع بالأمر:

```
git clone username@hostname:/path/to/repository
```

بعد نسخ الملفات إلى جهاز العميل، يمكنه تعديلها ثم إيداعها ومشاركتها بالأوامر:

```
cd /path/to/repository
# Edit some files
# Commit all changes to the local version of the repository
git commit -a
# Push changes to the server's version of the repository
git push origin master
```

د. تثبيت خادوم Gitolite

على الرغم من أنّ ما سبق كافٍ لإنشاء ونسخ وتعديل المستودعات، لكن المستخدمين الذين يريدون تثبيت git على خادوم سيريدون عمومًا إنجاز المهام في git كنظام إدارة التحكم بالأكواد المصدرية تقليدي؛ وعند وجود عدّة مستخدمين وامتيازات وصول لهم، فالحل الأمثل هو تثبيت Gitolite كما يلي:

```
sudo apt-get install gitolite
```

ضبط Gitolite

ضبط خادوم Gitolite مختلف قليلًا عن معظم الخواديم في الأنظمة الشبيهة بِيونكس؛ فبدلًا من ملفات الضبط التقليدية في /etc/، فإن Gitolite يُخزِّن الضبط في مستودع git؛ أول خطوة لضبط تثبيت جديد هي السماح بالوصول إلى مستودع الضبط.

أولًا، علينا إنشاء مستخدم لأجل Gitolite لكي نصل إليه عبره:

```
sudo adduser --system --shell /bin/bash --group \
--disabled-password --home /home/git git
```

سنترك الآن Gitolite لكي يعرف عن مفتاح SSH العمومي لمدير المستودع؛ هنا نفترض أن المستخدم الحالي هو مدير المستودع؛ إذا لم تضبط مفتاح SSH بعد، فراجع الفصل السادس لمزيدٍ من التفاصيل:

```
cp ~/.ssh/id_rsa.pub /tmp/$(whoami).pub
```

لنبدِّل إلى المستخدم git ونستورد مفتاح المدير إلى Gitolite:

```
sudo su - git
gl-setup /tmp/*.pub
```

سيسمح Gitolite لك بعمل تغيرات مبدئية لضبطه أثناء عملية الإعداد؛ يمكنك الآن نسخ وتعديل مستودع ضبط Gitolite من المستخدم المدير (المستخدم الذي استوردت مفتاح SSH العمومي الخاص به)؛ عُد إلى ذاك المستخدم، ثم انسخ مستودع الضبط:

```
exit
git clone git@$IP_ADDRESS:gitolite-admin.git
cd gitolite-admin
```

المجلد gitolite-admin فيه مجلدين فرعيين، المجلد «conf» و «keydir»؛ ملفات الضبط موجودة في مجلد conf، ويحتوي مجلد keydir على مفاتيح SSH العمومية للمستخدم.

إدارة مستخدمي ومستودعات Gitolite

إضافة مستخدمين جدد إلى Gitolite هي عملية سهلة: احصل على مفتاح SSH العمومي لهم ثم أضفه إلى مجلد keydir بالاسم USERNAME.pub، لاحظ أن أسماء مستخدمي Gitolite لا تطابق بالضرورة أسماء مستخدمي النظام، حيث تُستخدَم أسمائهم في ملف ضبط Gitolite فقط، وذلك لإدارة التحكم بالوصول؛ وبشكل مشابه، يمكن حذف المستخدمين بحذف ملف المفتاح العمومي الخاص بهم؛ ولا تنسَ أن تودع التغييرات وتدفعها إلى خادوم git بعد كل تعديل:

```
git commit -a
git push origin master
```

تُدار المستودعات بتعديل الملف conf/gitolite.conf؛ الشكل العام له هو قيود مفصولة بفراغات تُحدِّد ببساطة قائمةً بالمستودعات ثم بعض قواعد الوصول؛ ما يلي هو المثال الافتراضي لهذا الملف:

```
repo        gitolite-admin
            RW+        =      admin
            R          =      alice
repo        project1
            RW+        =      alice
            RW         =      bob
            R          =      denise
```

استخدام خادومك

لاستخدام الخادوم المُنشَأ حديثًا، يجب أن يستورد مدير Gitolite مفاتيح المستخدمين العمومية إلى مستودع ضبط Gitolite، ثم يمكنهم الوصول إلى أي مستودع لهم حق الوصول إليه عبر الأمر الآتي:

```
git clone git@$SERVER_IP:$PROJECT_NAME.git
```

أو إضافة مشروع في الخادوم عن بعد:

```
git remote add gitolite git@$SERVER_IP:$PROJECT_NAME.git
```

٣. نظام Subversion

إن Subversion هو نظام إدارة إصدارات مفتوح المصدر؛ يمكنك باستخدام Subversion أن تُسجِّل تاريخ كل الملفات المصدرية والمستندات؛ حيث يدير الملفات والمجلدات مع مرور الزمن. توضع شجرة من الملفات في مستودع مركزي، هذا المستودع يشبه كثيرًا خادوم الملفات العادي، عدا أنه «يتذكر» كل تعديل جرى على الملفات والمجلدات.

أ. التثبيت

للوصول إلى مستودع Subversion عبر بروتوكول HTTP، يجب عليك تثبيت وضبط خادوم ويب، أُثبِتَ عمل Subversion مع أباتشي؛ الرجاء العودة إلى القسم الخاص بإعداد خادوم أباتشي في الفصل الحادي عشر لمزيدٍ من المعلومات؛ للوصول إلى مستودع Subversion باستخدام بروتوكول HTTPS، فثبّت واضبط الشهادة الرقمية في خادوم أباتشي.

عليك تنفيذ الأمر الآتي في الطرفية لتثبيت Subversion:

```
sudo apt-get install subversion libapache2-svn
```

ب. ضبط الخادوم

يشرح هذا القسم كيفية إنشاء مستودع Subversion، والوصول إلى المشروع.

إنشاء مستودع Subversion

يمكن إنشاء مستودع Subversion بتنفيذ الأمر الآتي في الطرفية:

```
svnadmin create /path/to/repos/project
```

استيراد الملفات

تستطيع استيراد الملفات إلى المستودع بعد أن تُنشِئه؛ أدخِل الأمر الآتي في الطرفية لاستيراد مجلد:

```
svn import /path/to/import/directory \
file:///path/to/repos/project
```

ج. طرق الوصول

يمكن الوصول إلى مستودعات Subversion (السحب [checked out]) بطرقٍ مختلفة على الجهاز المحلي أو عبر بروتوكولات الشبكة المختلفة؛ لكن مكان المستودع (repository location) هو دائمًا عنوان URL؛ الجدول الآتي يحتوي على أنماط URL المختلفة لمختلف طرق الوصول.

الجدول ١٧-١: طرق الوصول إلى Subversion

النمط	طريقة الوصول
file://	الوصول المباشر إلى المستودع على القرص الصلب.
http://	الوصول عبر بروتوكول WebDAV في خادوم أباتشي يعمل بوجود Subversion.
https://	مثل النمط http:// لكن بتشفير SSL.
svn://	الوصول عبر بروتوكول خاص إلى خادوم svnserve.
svn+ssh://	مثل svn:// لكن عبر نفق SSH.

سنرى -في هذا القسم- كيفية ضبط Subversion لكل طرق الوصول السابقة؛ سنشرح هنا الأساسيات، رجاءً عُد إلى كتاب «SVN book» لتفاصيل استخدام متقدمة.

الوصول المباشر إلى المستودع

هذه هي أبسط طرق الوصول؛ لا تحتاج إلى أي خادوم Subversion يعمل؛ تُستخدَم هذه الطريقة للوصول إلى Subversion من نفس الجهاز؛ شكل الأمر المُدخَل في سطر الأوامر هو:

```
svn co file:///path/to/repos/project
```

أو:

```
svn co file://localhost/path/to/repos/project
```

ملاحظة: إن لم تحدد اسم المضيف، فهنالك ثلاث خطوط مائلة (///) حيث اثنتين منها للبروتوكول بالإضافة إلى الخط المائل في أول المسار؛ إذا حددت اسم المضيف، فسيكون هنالك خطين مائلين فقط.

تعتمد أذونات المستودع على أذونات نظام الملفات؛ إذا امتلك المستخدم إذن القراءة والكتابة، فيمكنه السحب من المستودع أو الإيداع إليه.

الوصول عبر بروتوكول WebDAV (http://)

يجب عليك ضبط خادوم أباتشي للوصول إلى مستودع Subversion عبر بروتوكول WebDAV؛ أضف الأسطر الآتية بين العنصرين <VirtualHost> و </VirtualHost> في ملف

/etc/apache2/sites-available/default؛ أو ملف VirtualHost آخر:

```
<Location /svn>
  DAV svn
  SVNPath /home/svn
  AuthType Basic
  AuthName "Your repository name"
  AuthUserFile /etc/subversion/passwd
  Require valid-user
</Location>
```

ملاحظة: يفترض الضبط السابق أن مستودعات Subversion موجودةٌ في مجلد /home/svn باستخدام الأمر svnadmin؛ ويملك مستخدم HTTP امتيازات وصول كافية على تلك الملفات، ويمكن الوصول إليها عبر الوصلة http://hostname/svn/repos_name.

التغيير السابق في ضبط أباتشي يتطلب إعادة تحميل الخدمة، وذلك بالأمر الآتي:

```
sudo service apache2 reload
```

لاستيراد أو إيداع ملفات إلى مستودع Subversion عبر HTTP، فيجب أن يكون المستودع مملوكًا من مستخدم HTTP؛ يكون مستخدم HTTP عادةً في أنظمة أوبنتو هو www-data؛ أدخِل الأمر الآتي في الطرفية لتغيير ملكية ملفات المستودع:

```
sudo chown -R www-data:www-data /path/to/repos
```

ملاحظة: بتغيير ملكية المستودع إلى www-data، فلن تتمكن من استيراد أو إيداع الملفات في المستودع بالأمر svn import file:/// عبر أي مستخدم عدا المستخدم www-data.

عليك الآن إنشاء الملف /etc/subversion/passwd الذي يحتوي معلومات استيثاق المستخدم؛ نفِّذ الأمر الآتي في الطرفية لإنشاء الملف (الذي سيُنشِئ الملف ويضيف أول مستخدم):

```
sudo htpasswd -c /etc/subversion/passwd user_name
```

لإضافة مستخدمين آخرين، احذف الخيار c-، حيث يستبدل هذا الخيار الملفَ القديم؛ واستخدم الشكل الآتي عوضًا عنه:

```
sudo htpasswd /etc/subversion/passwd user_name
```

سيُضاف المستخدم بعد إدخالك لكلمة المرور بنجاح؛ يمكنك الآن الوصول إلى المستودع بتنفيذ الأمر الآتي:

```
svn co http://servername/svn
```

تحذير: ستُنقل كلمة المرور كنص واضح، إذا كنت قلقًا على التجسس على كلمة المرور، فمن المستحسن استخدام تشفير SSL، اقرأ القسم الآتي للتفاصيل.

الوصول إلى بروتوكول WebDAV عبر اتصال SSL مشفر (//:https)

الوصول إلى مستودع Subversion عبر بروتوكول WebDAV مع تشفير SSL يشبه كثيرًا الوصول إلى //:http عدا أنه عليك تثبيت وضبط الشهادة الرقمية في خادوم أباتشي؛ أضف الضبط السابق إلى ملف /etc/apache2/sites-available/default-ssl.conf لاستخدام SSL مع Subversion؛ راجع الفصل الحادي عشر للمزيد من المعلومات حول ضبط أباتشي مع SSL.

يمكنك تثبيت شهادة رقمية مُصدَرَة من سلطة توقيع الشهادات؛ أو يمكنك تثبيت شهادتك الموقعة ذاتيًا.

تفترض هذه الخطوة أنك ثبتت وضبطت شهادةً رقميةً في خادوم أباتشي؛ راجع الأوامر في القسم السابق للوصول إلى مستودع Subversion، حيث أنَّ الخطوات متماثلة تمامًا عدا البروتوكول، حيث عليك استخدام //:https للوصول إلى مستودع Subversion.

الوصول عبر بروتوكول خاص

يمكنك ضبط التحكم بالوصول بعد إنشاء مستودع Subversion؛ تستطيع تعديل الملف /path/to/repos/project/conf/svnserve.conf لضبط التحكم بالوصول؛ على سبيل المثال، يمكنك إزالة التعليق عن الأسطر الآتية في ملف الضبط لضبط الاستيثاق:

```
# [general]
# password-db = passwd
```

بعد إزالة التعليق عن السطرين السابقين، يمكنك إدارة قائمة المستخدمين في ملف passwd، لذلك عدِّل ملف passwd في نفس المجلد وأضف مستخدمًا جديدًا كما يلي:

```
username = password
```

للوصول إلى Subversion عبر البروتوكول الخاص //:svn؛ من الجهاز نفسه أو من جهاز آخر، تستطيع تشغيل svnserver بالأمر svnserve؛ الذي يكون شكله العام كما يلي:

```
svnserve -d --foreground -r /path/to/repos
# -d -- daemon mode
# --foreground -- run in foreground (useful for debugging)
# -r -- root of directory to serve
```

سيبدأ Subversion بالاستماع إلى المنفذ الافتراضي (٣٦٩٠) بعد تنفيذ الأمر السابق؛ عليك تنفيذ الأمر الآتي من الطرفية للوصول إلى مستودع البرنامج:

```
svn co svn://hostname/project project --username user_name
```

وبناءً على إعدادات الخادوم، قد يُطلَب منك توفير كلمة مرور؛ وبعد أن تستوثق، فسيُسحب الكود من مستودع Subversion. ولمزامنة مستودع المشروع مع نسخة محلية، يمكنك تنفيذ الأمر الفرعي update؛ الشكل العام للأمر المُدخَل إلى الطرفية هو كما يلي:

```
cd project_dir; svn update
```

للمزيد من التفاصيل حول استخدام كل أمر فرعي من أوامر Subversion، يمكنك الرجوع إلى الدليل؛ على سبيل المثال، لتعلم المزيد عن الأمر co (أي السحب checkout)، رجاءً نفِّذ الأمر الآتي من الطرفية:

```
svn co help
```

الوصول عبر البروتوكول الخاص مع تشفير SSL (//:svn+ssh)

طريقة ضبط وتشغيل الخادوم هي نفسها في طريقة //:svn؛ يفترض هذا القسم أنك اتبعت الخطوة السابقة وبدأت خادوم Subversion باستخدام svnserve.

يُفترَض أيضًا أنه لديك خادوم ssh في ذاك الجهاز ويسمح للاتصالات القادمة؛ للتأكد من ذلك، رجاءً جرِّب تسجيل الدخول إلى ذاك الحاسوب باستخدام ssh، إذا استطعت الدخول فإن كل شيء على ما يرام؛ وإلا فعليك حلّ المشكلة قبل الإكمال.

البروتوكول //:svn+ssh يُستخدَم للوصول إلى مستودع Subversion باستخدام تشفير SSL؛ البيانات المنقولة في هذه الطريقة مشفرة، وللوصول إلى مستودع المشروع (للسحب على سبيل المثال)؛ فعليك استخدام الصيغة الآتية:

```
svn co svn+ssh://hostname/var/svn/repos/project
```

ملاحظة: عليك تحديد مسار كامل path/to/repos/project/ للوصول إلى مستودع Subversion باستخدام طريقة الوصول هذه.

قد تُسأل عن كلمة المرور اعتمادًا على ضبط الخادوم؛ إذ عليك إدخال كلمة المرور التي تستخدمها للوصول عبر ssh؛ وبعد أن يستوثق منك الخادوم، فيمكن سحب الكود من مستودع Subversion.

٤. نظام CVS

إن CVS هو خادوم تحكم بالإصدارات؛ تستطيع استخدامه لتسجيل تاريخ ملفات المصدر.

ا. التثبيت

نفِّذ الأمر الآتي في الطرفية لتثبيت CVS:

```
sudo apt-get install cvs
```

بعد تثبيت cvs، يجب عليك تثبيت xinetd لتشغيل أو إيقاف خادوم cvs؛ وذلك بإدخال الأمر الآتي في الطرفية:

```
sudo apt-get install xinetd
```

ب. الضبط

بعد أن تثبت cvs، فإنه سيُهيّء مستودعًا تلقائيًا؛ يقبع المستودع افتراضيًّا في مجلد /srv/cvs؛ ويمكنك تغيير هذا المسار بتنفيذ الأمر الآتي:

```
cvs -d /your/new/cvs/repo init
```

تستطيع ضبط xinetd لبدء خادوم CVS بعد أن يُضبَط المستودع الابتدائي؛ يمكنك نسخ الأسطر الآتية إلى ملف /etc/xinetd.d/cvspserver:

```
service cvspserver
{
      port = 2401
      socket_type = stream
      protocol = tcp
      user = root
      wait = no
      type = UNLISTED
      server = /usr/bin/cvs
      server_args = -f --allow-root /srv/cvs pserver
      disable = no
}
```

ملاحظة: تأكد أن تعدِّل المستودع إذا غيرت مجلد المستودع الافتراضي (/srv/cvs).

بعد أن تضبط xinetd؛ يمكنك بدء خادوم CVS بإدخال الأمر الآتي:

```
sudo service xinetd restart
```

يمكنك التأكد من عمل خادوم CVS بإدخال الأمر الآتي:

```
sudo netstat -tap | grep cvs
```

يجب أن ترى مخرجاتٍ شبيهةً بالمخرجات الآتية بعد تنفيذ الأمر السابق:

```
tcp        0      0 *:cvspserver                 *:* LISTEN
```

من هنا يمكنك المتابعة في إضافة المستخدمين والمشاريع الجديدة وإدارة خادوم CVS.

تحذير: يسمح CVS للمستخدم بإضافة مستخدمين بشكل مستقل عن نظام التشغيل؛ وربما أسهل طريقة هي استخدام مستخدمي لينُكس لخادوم CVS، على الرغم من أن لها مساوئ أمنية؛ راجع دليل CVS للتفاصيل.

ج. إضافة مشاريع

يشرح هذا القسم كيفية إضافة مشاريع جديدة إلى مستودع CVS؛ أنشِئ مجلدًا وأضف المستندات والملفات المصدرية إليه؛ ثم نفِّذ الأمر الآتي لإضافة هذا المشروع إلى مستودع CVS:

```
cd your/project
cvs -d :pserver:username@hostname.com:/srv/cvs import -m \
"Importing my project to CVS repository" . new_project start
```

تنويه: يمكن استخدام متغير البيئة CVSROOT لتخزين المجلد الجذر لخادوم CVS؛ يمكنك تجنب استخدام الخيار d- في أمر cvs السابق بعد أن «تُصدِّر» (export) متغير البيئة CVSROOT.

السلسلة النصية new_project هي وسم «vendor»، و start هي وسم «release» لا يخدمان أي هدف في هذا السياق، لكن ولما كان خادوم CVS يتطلب وجودهما؛ فيجب أن تضعهما.

تحذير: عندما تضيف مشروعًا جديدًا، فيجب أن يملك مستخدم CVS إذن الوصول إلى مستودع CVS (/srv/cvs)؛ تملك المجموعة src افتراضيًا إذن الكتابة إلى مستودع CVS؛ لذلك تستطيع إضافة المستخدم إلى هذه المجموعة، ثم سيستطيع إضافة وإدارة المشاريع في مستودع CVS.

---

٥. مصادر

- صفحة Bazaar الرئيسية.
- Launchpad.
- صفحة Git الرئيسية.
- صفحة مشروع Gitolite.
- صفحة Subversion الرئيسية.
- كتاب Subversion.
- دليل CVS.
- صفحة ويكي أوبنتو «Easy Bazaar».
- صفحة ويكي أوبنتو «Subversion».

١٨

سامبا

تتألف شبكات الحواسيب عادةً من خليط من أنظمة التشغيل، وعلى الرغم من أن شبكة مبنية كاملًا من حواسيب بأنظمة خادوم وسطح مكتب أوبنتو يمكن أن تكون ذات فائدة عظيمة؛ إلّا أن بعض بيئات الشبكة يجب أن تحتوي على أنظمة أوبنتو ومايكروسوفت ويندوز تعمل سويةً بتناغم؛ سيقدم هذا الجزء من الكتاب المبادئ الأساسية والأدوات المستخدم في ضبط خادوم أوبنتو لمشاركة موارد الشبكة مع حواسيب ويندوز.

١. مقدمة

يتطلب التواصل الشبكي الناجح بين خادوم أوبنتو وعملاء ويندوز توفير ودمج الخدمات الشائعة لبيئات ويندوز؛ تساعد مثل هذه الخدمات في مشاركة البيانات والمعلومات عن الحواسيب والمستخدمين الموجودين في الشبكة، ويمكن تصنيفها تحت ثلاثة تصنيفات للوظائف التي تؤديها:

- خدمات مشاركة الملفات والطابعات. استخدام بروتوكول «Server Message Block» (اختصارًا SMB) لتسهيل مشاركة الملفات والمجلدات والأقراص ومشاركة الطابعات عبر الشبكة.
- خدمات الدليل (Directory). مشاركة المعلومات الحيوية عن الحواسيب ومستخدمي الشبكة باستخدام تقنيات مثل LDAP و ®Microsoft Active Directory.
- الاستيثاق والوصول. التحقق من هوية حاسوب أو مستخدم للشبكة وتحديد المعلومات التي يُصرَّح للحاسوب أو المستخدم بالوصول إليها عبر تقنيات مثل أذونات الملفات، وسياسات المجموعات، وخدمة الاستيثاق Kerberos.

لحسن الحظ، يمكن لخادوم أوبنتو توفير هذه الخدمات إلى عملاء ويندوز ومشاركة موارد الشبكة معهم؛ واحد من أهم البرمجيات التي يتضمنها نظام أوبنتو للتعامل الشبكي مع ويندوز هو مجموعة أدوات وتطبيقات خادوم SMB المُسمى سامبا.

سيقدم هذا القسم من الكتاب بعض حالات استخدام سامبا الشائعة، وطريقة تثبيت وضبط الحزم الضرورية؛ تفاصيلٌ إضافيةٌ يمكن العثور عليها في موقع سامبا.

٢. خادوم الملفات

أحد أشهر الطرق للتواصل الشبكي بين أوبنتو وويندوز هو ضبط سامبا كخادوم ملفات؛ يشرح هذا القسم طريقة ضبط خادوم سامبا لمشاركة الملفات مع عملاء ويندوز.

سيُضبَط الخادوم لمشاركة الملفات مع أي عميل على الشبكة دون طلب كلمة مرور منه؛ إذا كانت بيئتك تتطلب متحكمات بالوصول أكثر تقييدًا ، فراجع القسم «تأمين خادوم سامبا لتخديم الملفات والطباعة».

ا. التثبيت

أول خطوة هي تثبيت حزمة samba؛ وذلك بإدخال الأمر الآتي من الطرفية:

```
sudo apt-get install samba
```

هذا كل ما عليك فعله! يجب أن تكون الآن جاهزًا لضبط سامبا لمشاركة الملفات.

ب. الضبط

ملف ضبط سامبا الرئيسي موجودٌ في /etc/samba/smb.conf؛ توجد كميةٌ كبيرةٌ من التعليقات في ملف الضبط لتوثيق مختلف تعليمات الضبط.

ملاحظة: لا تُضمَّن جميع الخيارات المتوفرة في ملف الضبط الافتراضي؛ راجع صفحة الدليل للملف smb.conf أو مجموعة «Samba HOWTO».

أولًا، عدِّل الأزواج المفتاح/القيمة في القسم [global] من ملف /etc/samba/smb.conf:

```
workgroup = EXAMPLE
...
security = user
```

المعامل security موجودٌ في أسفل قسم [global]، ويوجد قبله تعليق افتراضيًا؛ غيِّر أيضًا القيمة EXAMPLE إلى قيمة تلائم بيئتك.

أنشِئ قسمًا جديدًا في نهاية الملف -أو أزل التعليق عن أحد الأمثلة- للمجلد الذي تريد أن تشاركه:

```
[share]
      comment = Ubuntu File Server Share
      path = /srv/samba/share
      browsable = yes
      guest ok = yes
      read only = no
      create mask = 0755
```

- comment: وصف قصير عن المشاركة، عدِّله ليناسب احتياجاتك.
- path: مسار المجلد الذي تريد مشاركته؛ يستخدم هذا المثال /srv/samba/sharename لأنه وفقًا لمعيار هيكلة نظام الملفات (Filesystem Hierarchy Standard اختصارًا FHS)، فإن /srv هو مكان تخزين البيانات التي ستُخدَّم؛ ويمكن (تقنيًا) أن تكون مشاركات سامبا في أي مكان في نظام الملفات لطالما كانت الأذونات صحيحةً، لكن الالتزام بالمعايير أمرٌ حسن.

- browsable: يفعّل إمكانية تصفح عملاء ويندوز للمجلد باستخدام «مستكشف الملفات».

- guest ok: يسمح للعملاء بالاتصال إلى المشاركة دون توفير كلمة مرور.

- read only: تحديد إذا ما كانت المشاركة للقراءة فقط أم كان إذن الكتابة معطيًا؛ يُعطى إذن الكتابة فقط عندما تكون القيمة هي no (كما هو الحال في هذا المثال) إذا كانت القيمة yes، فإن الوصول للمشاركة سيكون للقراءة فقط.

- create mask: تحديد أذونات الملفات الجديدة عندما تُنشَأ.

بعد أن ضُبِطَ سامبا، فيجب إنشاء المجلد وتغيير الأذونات؛ وذلك بإدخال الأمر الآتي من الطرفية:

```
sudo mkdir -p /srv/samba/share
sudo chown nobody.nogroup /srv/samba/share/
```

ملاحظة: الخيار p- يخُبِر mkdir بأن يُنشِئ كامل شجرة المجلد إن لم تكن موجودةً.

في النهاية، أعد تشغيل خدمات samba لتفعيل الضبط الجديد:

```
sudo restart smbd
sudo restart nmbd
```

تحذير: يسمح الضبط السابق بالوصول لأي مستخدم في الشبكة المحلية، لضبط أكثر أمانًا راجع القسم «تأمين خادوم سامبا لتخديم الملفات والطباعة».

تستطيع الآن من عميل ويندوز أن تكون قادرًا على تصفح خادوم أوبنتو للملفات ورؤية مشاركة المجلد؛ إذا لم تظهر المشاركة عند عميلك تلقائيًا، فحاول أن تصل إلى الخادوم عبر عنوان IP الخاص به؛ مثلًا، 192.168.1.1\\ في نافذة مستكشف الملفات، حاول إنشاء مجلد من ويندوز للتحقق من أن كل شيء يعمل على ما يرام.

لمشاركة مجلدات إضافية، فأنشِئ ببساطة أقسام [dir] في /etc/samba/smb.conf وأعد تشغيل خدمة سامبا؛ عليك أن تتأكد أن المجلد الذي تريد مشاركته موجود فعلًا، والأذونات المُعطاة له صحيحة.

ملاحظة: المشاركة المُسماة «[share]» والمسار /srv/samba/share هما مجرد مثالين؛ عدِّل اسم ومسار المشاركة لملائمة بيئتك؛ فكرة جيدة هي تسمية اسم المشاركة باسم المجلد في نظام الملفات؛ مثال آخر سيكون مشاركةً باسم [qa] بمسار /srv/samba/qa.

ج. مصادر

- كتاب «Using Samba» من O'Reilly هو مصدر جيد للمعلومات.
- صفحة ويكي أوبنتو «Samba» فيها بعض المعلومات.

٣. خادوم سامبا للطباعة

استخدام شائع آخر لخادوم سامبا هو ضبطه لمشاركة الطابعات المثبتة إما محليًا أو عبر الشبكة على خادوم أوبنتو؛ وبآليةٍ شبيهةٍ بالآلية في قسم «خادوم ملفات سامبا»، سيضبط هذا القسم سامبا للسماح لأي عميل في الشبكة المحلية باستخدام الطابعات المثبتة دون طلب اسم مستخدم وكلمة مرور.

لضبط أكثر أمانًا، راجع القسم الآتي «تأمين خادوم سامبا لتخديم الملفات والطباعة».

ا. التثبيت

قبل تثبيت وضبط سامبا، من الأفضل أن يكون لديك تثبيت CUPS يعمل جيدًا، راجع القسم «خادوم الطباعة CUPS» في الفصل الرابع عشر لمزيدٍ من المعلومات.

أدخِل ما يلي في الطرفية لتثبيت حزمة samba:

```
sudo apt-get install samba
```

ب. الضبط

بعد تثبيت سامبا، عدِّل الملف /etc/samba/smb.conf مغيّرًا الخاصية workgroup إلى القيمة الملائمة لشبكتك، وعدِّل قيمة security إلى user:

```
workgroup = EXAMPLE
...
security = user
```

عدِّل قيمة الخيار guest ok إلى yes في قسم [printers]:

```
browsable = yes
guest ok = yes
```

أعد تشغيل سامبا بعد إتمام تعديل ملف smb.conf:

```
sudo restart smbd
sudo restart nmbd
```

سيشارك ضبط سامبا الافتراضي كل الطابعات المثبتة، كل ما عليك فعله هو تثبيت الطابعة محليًا على عملاء ويندوز.

ج. مصادر

- راجع موقع CUPS لمزيد من المعلومات حول ضبط CUPS.

٤. تأمين خادوم سامبا لتخديم الملفات والطباعة

ا. أنماط حماية سامبا

هنالك مستويان أمنيان متوفران لبروتوكول الشبكة «نظام ملفات الإنترنت الشائع» (Common Internet Filesystem اختصارًا CIFS) هما user-level و share-level؛ نمط الحماية المستخدم في سامبا يسمح بمرونة زائدة، موفرًا أربع طرق لاستخدام الحماية من مستوى user-level وطريقة لاستخدام share-level:

- النمط security=user: يتطلب من العملاء توفير اسم مستخدم وكلمة مرور للاتصال إلى المشاركات؛ حسابات المستخدمين في سامبا منفصلة عن حسابات مستخدمي النظام، لكن الحزمة libpam-smbpass ستُزامن مستخدمي النظام وكلمات مرورهم مع قاعدة بيانات مستخدمي سامبا.

- النمط security=domain: هذا النمط يسمح لخادوم سامبا بأن يَظهر لعملاء ويندوز كالمتحكم الرئيسي بالنطاق (Primary Domain Controller اختصارًا PDC)، أو متحكم الاحتياطي بالنطاق (Backup Domain Controller اختصارًا BDC)، أو خادوم عضو في النطاق (Domain Member Server اختصارًا DMS)، راجع القسم «استخدام سامبا كمتحكم بالنطاق» للمزيد من المعلومات.

- النمط security=ADS: السماح لخادوم سامبا بالانضمام إلى نطاق Active Directory كعضو أصلي (native member)؛ راجع القسم «دمج سامبا مع Active Directory» للتفاصيل.

- النمط security=server: هذا النمط تُرِك قبل أن يتمكن سامبا من أن يصبح خادومًا عضوًا، وبسبب بعض المشاكل الأمنية، فلا يجب أن يُستخدَم؛ راجع قسم «Server Security» من دليل سامبا لمزيدٍ من التفاصيل.
- النمط security=share: يسمح لجميع العملاء بالاتصال إلى المشاركات دون توفير اسم مستخدم وكلمة مرور.

يعتمد اختيارك لنمط الحماية بالبيئة التي تعمل فيها وما الذي تريد من خادوم سامبا أن يُنجزه.

النمط Security = User

سيعيد هذا القسم ضبط خادوم سامبا لمشاركة الملفات والطباعة من القسمين السابقين، كي يتطلب الاستيثاق.

أولًا، ثبِّت الحزمة libpam-smbpass التي ستزامن مستخدمي النظام إلى قاعدة بيانات مستخدمي سامبا:

```
sudo apt-get install libpam-smbpass
```

ملاحظة: لو اخترت مهمة «Samba Server» أثناء التثبيت، فستكون الحزمة libpam-smbpass مثبَّتةً مسبقًا.

عدِّل الملف /etc/samba/smb.conf، وعدِّل ما يلي في قسم [share]:

```
guest ok = no
```

في النهاية، أعد تشغيل سامبا لكي تأخذ الإعدادات الجديدة مفعولها:

```
sudo restart smbd
sudo restart nmbd
```

سيُطلَب منك الآن إدخال اسم مستخدم وكلمة مرور عند الاتصال إلى المجلدات المشاركة أو الطابعات.

ملاحظة: إذا اخترت ربط قرص شبكي للمشاركة، فعليك تفعيل الحقل «Reconnect at Logon»؛ مما يجعله يطلب اسم المستخدم وكلمة المرور مرةً واحدةً فقط، على الأقل إلى أن تُغيَّر كلمة المرور.

ب. تأمين المشاركة

هنالك عدِّة خيارات متوفرة لزيادة الحماية لمشاركات المجلدات المنفصلة؛ وباستخدام مثال «[share]»، فسيشرح هذا القسم بعض الخيارات الشائعة.

المجموعات

تُعرِّف المجموعات تشكيلةً من الحواسيب أو المستخدمين الذي يملكون وصولًا متكررًا إلى مورد شبكي معين؛ على سبيل المثال، إذا عُرِّفت المجموعة qa وكانت تحتوي على المستخدمين freda، و danika، و rob؛ ومجموعة ثانية هي support تحتوي على المستخدمين danika، و jeremy، و vincent؛ وضُبِط مورد شبكي معيّن للسماح بالوصول إلى المجموعة qa، والذي بدوره سيمنح المستخدمين freda، و danika، و rob وصولًا لكن ليس jeremy أو vincent؛ ولما كان المستخدم danika ينتمي إلى كلي المجموعتين qa و support؛ فسيتمكن من الوصول إلى الموارد التي يُسمَح لكلا المجموعتين بالوصول إليها، بينما كل المستخدمين الباقيين سيقيدون بالموارد التي تسمح بوصول مجموعتهم إليها.

يبحث سامبا عن المجموعات في النظام المحلي المُعرَّفة في etc/group/ ليحدد أي مستخدم ينتمي إلى أي مجموعة؛ للمزيد من المعلومات حول إضافة أو إزالة المستخدمين من المجموعات، راجع القسم «إضافة وحذف المستخدمين» من الفصل التاسع.

عند تعريف المجموعات في ملف ضبط سامبا، etc/samba/smb.conf/؛ فإن الصيغة المتعارف عليها هي بدء اسم المجموعة بالرمز «@»؛ على سبيل المثال، إذا أردت تعريف مجموعة مسماة sysadmin في قسم محدد من ملف etc/samba/smb.conf/، فعليك إدخال اسم المجموعة ‎@sysadmin.

أذونات الملف

تُعرِّف أذونات الملف الحقوق المحددة التي يملكها حاسوب أو مستخدم على مجلد أو ملف أو مجموعة ملفات؛ يمكن تعريف هذه الأذونات بتعديل الملف /etc/samba/smb.conf وتحديد الأذونات لمشاركة ملف معيّن.

على سبيل المثال، لو عَرَّفتَ مشاركة سامبا اسمها share وأردت إعطاء أذونات «للقراءة فقط» لمجموعة المستخدم qa؛ لكنك تريد السماح بالكتابة لمجموعة اسمها sysadmin ومستخدم اسمه vincent، فعليك تعديل الملف /etc/samba/smb.conf وإضافة القيود الآتية تحت قيد [share]:

```
read list = @qa
write list = @sysadmin, vincent
```

طريقة أخرى لضبط الأذونات في سامبا هي التصريح عن أذونات «إدارية» لمورد معيّن مُشارَك؛ حيث يمكن للمستخدمين الذي يملكون أذونات إدارية قراءة أو كتابة أو تعديل أيّة معلومات موجودة في المورد الذي أُعطي ذاك المستخدم أذوناتٍ إدارية خاصة عليه.

على سبيل المثال، إذا أردت إعطاء المستخدم melissa أذوناتٍ إدارية للمشاركة share، فعليك تعديل الملف /etc/samba/smb.conf وإضافة الأسطر الآتية تحت القيد [share]:

```
admin users = melissa
```

بعد تعديل الملف /etc/samba/smb.conf، أعد تشغيل سامبا كي تأخذ التعديلات مجراها:

```
sudo restart smbd
sudo restart nmbd
```

ملاحظة: لكي تعمل «read list» و «write list»، لا يجب أن يكون نمط حماية المستخدم في سامبا مضبوطًا إلى security = share.

ضُبِط سامبا الآن ليحدد أيّة مجموعات تملك الوصول إلى مجلد مُشارَك، يجب الآن تحديث أذونات نظام الملفات.

نظام أذونات لينُكس التقليدي لا يترابط جيدًا مع قوائم التحكم بالوصول في ويندوز NT (Windows NT Access Control Lists اختصارًا ACLs)؛ لحسن الحظ، توجد POSIX ACLs في خواديم أوبنتو موفرةً تحكمًا أفضل؛ على سبيل المثال، للسماح باستخدام ACLs على /srv بنظام ملفات EXT3، فعدِّل الملف /etc/fstab وأضف الخيار acl كما يلي:

```
UUID=66bcdd2e-8861-4fb0-b7e4-e61c569fe17d /srv ext3
noatime,relatime,acl 0      1
```

ثم أعد وصل القسم:

```
sudo mount -v -o remount /srv
```

ملاحظة: تفترض الأوامر السابقة أن /srv على قسمٍ مختلف؛ إذا كان /srv، أو أي مسار آخر تختار مشاركته، هو جزء من قسم الجذر /، فربما عليك إعادة إقلاع النظام.

لمطابقة ضبط سامبا، فستُعطى المجموعة sysadmin أذونات القراءة والكتابة والتنفيذ إلى /srv/samba/share، وستُعطى المجموعة qa إذنَيّ القراءة والتنفيذ؛ وستُملَك الملفات من المستخدم melissa. أدخِل الأوامر الآتية في الطرفية:

```
sudo chown -R melissa /srv/samba/share/
sudo chgrp -R sysadmin /srv/samba/share/
sudo setfacl -R -m g:qa:rx /srv/samba/share/
```

ملاحظة: الأمر setfacl السابق يعطي أذونات التنفيذ إلى جميع الملفات في المجلد /srv/samba/share، ربما يكون أو لا يكون هذا ما تريده.

الآن من عميل ويندوز، يجب أن تلاحظ تطبيق الأذونات الجديدة للملف؛ راجع صفحات دليل acl و setfacl لمزيد من المعلومات حول POSIX ACLs.

ج. ملف ضبط سامبا لبرمجية AppArmor

يأتي أوبنتو مع وحدة الحماية AppArmor، الذي يوفر تحكمًا مقيّدًا للوصول؛ ملف الضبط الافتراضي الخاص ببرمجية AppArmor لخدمة سامبا يجب أن يلائم ضبطك، للمزيد من التفاصيل حول استخدام AppArmor راجع «الفصل التاسع - الحماية».

هنالك ملفات ضبط افتراضية لكلي /usr/sbin/smbd و /usr/sbin/nmbd (الملفات الثنائية لعفريت سامبا) كجزءٍ من حزمة apparmor-profiles؛ أدخِل الأمر الآتي من الطرفية لتثبيت الحزمة:

```
sudo apt-get install apparmor-profiles apparmor-utils
```

افتراضيًا، تكون ملفات الضبط لعفريتي smbd و nmbd في وضع «البناء» مما يسمح لخدمة سامبا بالعمل دون تعديل ملف الضبط، وستُسجَّل الأخطاء فقط؛ لجعل ملف ضبط smbd في وضع «الإجبار»، ولكي يعمل سامبا كما يجب، فيجب أن يُعدَّل ملف الضبط لتضمين المجلدات التي تمت مشاركتها.

عدِّل ملف /etc/apparmor.d/usr.sbin.smbd مضيفًا معلومات [share]:

```
/srv/samba/share/ r,
/srv/samba/share/** rwkix,
```

ضع الملف في وضع «الإجبار» وأعد تحميله:

```
sudo aa-enforce /usr/sbin/smbd
cat /etc/apparmor.d/usr.sbin.smbd | sudo apparmor_parser -r
```

يجب أن تكون قادرًا على قراءة وكتابة وتنفيذ الملفات في المجلد المُشارَك كالمعتاد، لكن smbd يملك الآن حق الوصول إلى الملفات والمجلدات المضبوطة فقط؛ تأكد من إضافة القيود لكل مجلد تضبط مشاركته في سامبا؛ وستسجل أيضًا أيّة أخطاء إلى /var/log/syslog.

د. مصادر

- الفصل الثامن عشر من «Samba HOWTO Collection» مخصصٌ للحماية.
- للمزيد من المعلومات حول Samba و ACLs، راجع الصفحة «Samba ACLs».
- راجع أيضًا صفحة ويكي أوبنتو «Samba».

٥. استخدام سامبا كمتحكم في النطاق

على الرغم من أن سامبا لا يمكن أن يكون Active Directory Primary Domain Controller (PDC)، لكن يمكن أن يُضبَط خادوم سامبا ليظهر كمتحكم من نمط Windows NT4؛ ميزة لهذا الضبط هي قابلية جعل تصاريح المستخدمين والحواسيب مركزية؛ يمكن أيضًا أن يَستخدم سامبا عدّة أنواع من السند الخلفي (backends) لتخزين بيانات المستخدم.

ا. متحكم رئيسي بالنطاق

يشرح هذا القسم طريقة ضبط سامبا ليعمل كمتحكم رئيسي بالنطاق (PDC) باستخدام السند الخلفي الافتراضي smbpasswd.

أولًا، ثبّت سامبا و libpam-smbpass لمزامنة حسابات المستخدمين؛ وذلك بإدخال الأمر الآتي في الطرفية:

```
sudo apt-get install samba libpam-smbpass
```

ثم اضبط سامبا بتعديل الملف /etc/samba/smb.conf؛ حيث يجب أن يُضبَط نمط security إلى user؛ ويجب أن تتعلق workgroup بمنظمتك:

```
workgroup = EXAMPLE
...
security = user
```

في قسم «Domains» المحاط بتعليقات، أضف أو أزل التعليق عمّا يلي (قُسِّم آخر سطر إلى قسمين ليتسع في عرض الصفحة):

```
domain logons = yes
logon path = \\%N\%U\profile
logon drive = H:
logon home = \\%N\%U
logon script = logon.cmd
add machine script = sudo /usr/sbin/useradd -N -g machines -c
↪ Machine -d /var/lib/samba -s /bin/false %u
```

ملاحظة: إذا أردت عدم استخدام «Roamin Profiles» فاترك الخيارين «logon home» و «logon path» مسبوقَين بتعليق.

- domain logons: يوفر خدمة netlogon مما يجعل سامبا يتصرف كمتحكم بالنطاق.
- logon path: يضع ملف profile الخاص بويندوز في مجلد المنزل للمستخدم؛ من الممكن ضبط مشاركة [profiles] ووضع كل ملفات profile في مجلد واحد.
- logon home: تحديد مكان مجلد المنزل.
- logon script: تحديد السكربت الذي يُشغَّل محليًا بعد أن يُسجِّل المستخدم دخوله؛ يجب أن يوضع السكربت في مشاركة [netlogon].
- add machine script: السكربت الذي يُنشِئ تلقائيًا الحساب Machine Trust الضروري لكي تنضم محطة العمل (workstation) إلى النطاق.

في هذا المثال، أُنشِئت المجموعة machines بالأداة addgroup؛ راجع الفصل التاسع قسم «إضافة وحذف المستخدمين» لمزيدٍ من التفاصيل.

أزل التعليق عن مشاركة [homes] للسماح بربط logon home:

```
[homes]
  comment = Home Directories
  browseable = no
  read only = no
  create mask = 0700
  directory mask = 0700
  valid users = %S
```

بعد أن يُضبَط كمتحكم بالنطاق، يجب أن تُضبَط الآن المشاركة [netlogon]، أزل التعليق عما يلي لتفعيل تلك المشاركة:

```
[netlogon]
  comment = Network Logon Service
  path = /srv/samba/netlogon
  guest ok = yes
  read only = yes
  share modes = no
```

ملاحظة: مسار مشاركة netlogon الافتراضي هو /home/samba/netlogon؛ لكن وفقًا لمعيار هيكلة نظام الملفات (FHS)، إن /srv هو المسار الصحيح للبيانات الموفرة من الخادوم.

أنشِئ الآن مجلد netlogon وملف سكربت logon.cmd فارغًا (حاليًا):

```
sudo mkdir -p /srv/samba/netlogon
sudo touch /srv/samba/netlogon/logon.cmd
```

يمكنك إدخال أوامر سكربت Windows Logon في ملف logon.cmd لتخصيص بيئة العميل.

أعد تشغيل سامبا لتفعيل المتحكم بالنطاق الجديد:

```
sudo restart smbd
sudo restart nmbd
```

في النهاية، هنالك بعض الأوامر الإضافية لضبط الحقوق الملائمة.

لما كان حساب الجذر معطلًا افتراضيًا، ولكي تنضم محطة عمل إلى النطاق، فيجب أن تُربَط مجموعة في النظام إلى مجموعة Windows Domain Admins؛ أدخِل الأمر الآتي الذي يستخدم الأداة net:

```
sudo net groupmap add ntgroup="Domain Admins" \
unixgroup=sysadmin rid=512 type=d
```

ملاحظة: عدِّل sysadmin إلى المجموعة التي تفضلها؛ وأيضًا يجب أن يكون المستخدم الذي ينضم إلى النطاق عضوًا في المجموعة sysadmin ومجموعة النظام admin، التي تسمح باستخدام sudo.

إذا لم يحصل المستخدم على تصاريح سامبا بعد؛ فيمكنك إضافتها باستخدام الأداة smbpasswd، لا تنسَ تعديل اسم sysadmin ليلائم نظامك:

```
sudo smbpasswd -a sysadmin
```

أيضًا، يجب أن تكون الحقوق المعطاة إلى مجموعة Domain Admins مُحدَّدةً للسماح لإضافة machine script (والوظائف الإدارية الأخرى) بأن تعمل؛ ويمكن فعل ذلك بالأمر:

```
net rpc rights grant -U sysadmin "EXAMPLE\Domain Admins" \
SeMachineAccountPrivilege SePrintOperatorPrivilege \
SeAddUsersPrivilege SeDiskOperatorPrivilege \
SeRemoteShutdownPrivilege
```

يجب أن تكون الآن قادرًا على ضم عملاء ويندوز إلى النطاق بنفس الطريقة التي ينضمون فيها إلى نطاق NT4 يعمل على خادوم ويندوز.

ب. متحكم احتياطي بالنطاق

بوجود متحكم رئيسي بالنطاق (PDC) في الشبكة، فمن الأفضل وجود متحكم احتياطي بالنطاق (BDC) أيضًا؛ مما يسمح باستيثاق العملاء في حال أصبح المتحكم الرئيسي غير متوفرٍ.

عندما تضبط سامبا كمتحكم احتياطي، فستحتاج إلى آلية لمزامنة معلومات الحسابات مع المتحكم الرئيسي؛ هنالك عدّة طرق لفعل ذلك تتضمن scp، أو rsync، أو باستخدام LDAP كسند passdb خلفي.

استخدام LDAP هو أكثر الطرق مرونةً لمزامنة معلومات الحسابات، لأن كلا المتحكمَين بالنطاق يستخدمان نفس المعلومات في الوقت الحقيقي؛ لكن إعداد خادوم LDAP هو أمرٌ زائد التعقيد لشبكة تحتوي عددًا قليلًا من حسابات المستخدمين والحواسيب؛ راجع القسم «استخدام سامبا مع LDAP» للتفاصيل.

أولًا، ثبِّت samba و libpam-smbpass، وذلك بإدخال الأمر الآتي في الطرفية:

```
sudo apt-get install samba libpam-smbpass
```

عدِّل الآن ملف /etc/samba/smb.conf وأزل التعليق عمّا يلي في قسم [global]:

```
workgroup = EXAMPLE
...
security = user
```

في قسم Domains المحاط بتعليق، أضف أو أزل التعليق عن:

```
domain logons = yes
domain master = no
```

تأكد أن المستخدم لديه الحقوق لقراءة الملفات في /var/lib/samba؛ على سبيل المثال، للسماح لمجموعة admin بنقل الملفات عبر scp، فأدخِل الأمر:

```
sudo chgrp -R admin /var/lib/samba
```

ثم، زامن حسابات المستخدمين، باستخدام scp لنسخ مجلد /var/lib/samba من PDC:

```
sudo scp -r username@pdc:/var/lib/samba /var/lib
```

ملاحظة: استبدل username باسم مستخدم صالح، و pdc باسم PDC أو عنوان IP له.

ثم في النهاية، أعِد تشغيل سامبا:

```
sudo restart smbd
sudo restart nmbd
```

يمكنك اختبار عمل متحكم النطاق الاحتياطي بإيقاف عفريت سامبا في PDC، ثم محاولة تسجيل الدخول من عميل ويندوز موجود في النطاق.

شيء آخر لتبقيه في بالك أنَّه إذا ضُبِط الخيار logon home إلى مجلد في PDC، فإذا أصبح PDC غير متوفرٍ، فإن الوصول إلى قرص المنزل للمستخدم سيصبح متعذرًا؛ لهذا السبب من الأفضل ضبط logon home ليقبع في خادوم ملفات منفصل عن PDC و BDC.

ج. مصادر

- الفصل الرابع والفصل الخامس من «Samba HOWTO Collection» يشرحان طريقة ضبط خادوم سامبا ليكون متحكمًا رئيسيًا واحتياطيًا بالنطاق على التوالي وبالترتيب.

٦. دمج سامبا مع Active Directory

ا. الوصول إلى مشاركة سامبا

استخدام آخر لخدمة سامبا هو الاندماج مع شبكة ويندوز موجودة مسبقًا، وبعد أن يصبح سامبا جزءًا من نطاق Active Directory، فيمكن لخدمة سامبا توفير خدمات مشاركة الملفات والطباعة إلى مستخدمي AD.

أبسط طريقة للانضمام إلى نطاق AD هي استخدام Likewise-open؛ لإرشادات تفصيلية، انظر إلى «Likewise Open Installation and Administration Guide».

بعد أن يصبح جزءًا في نطاق Active Directory؛ أدخِل الأمر الآتي في الطرفية:

```
sudo apt-get install samba smbfs smbclient
```

ثم عدِّل الملف /etc/samba/smb.conf مُغيِّرًا:

```
workgroup = EXAMPLE
...
security = ads
realm = EXAMPLE.COM
...
idmap backend = lwopen
idmap uid = 50-9999999999
idmap gid = 50-9999999999
```

أعد تشغيل سامبا لتأخذ التعديلات الجديدة تأثيرها:

```
sudo restart smbd
sudo restart nmbd
```

يجب أن تكون الآن قادرًا على الوصول إلى أي من مشاركات سامبا من عميل Windows؛ لكن للتأكد من إعطاء مستخدمي أو مجموعات AD الملائمة الوصول إلى مجلد مشترك؛ راجع القسم «تأمين خادوم سامبا لتخديم الملفات والطباعة» لمزيدٍ من التفاصيل.

ب. الوصول إلى مشاركة ويندوز

بعد أن أصبح خادوم سامبا جزءًا من نطاق Active Directory فتستطيع الوصول إلى أيّة مشاركات من خادوم ويندوز:

أدخِل الأمر الآتي في الطرفية لوصل مشاركة من ويندوز:

```
mount.cifs //fs01.example.com/share mount_point
```

من الممكن الوصول إلى مشاركات على حواسيب ليست جزءًا من نطاق AD، لكن يجب توفير اسم مستخدم وكلمة مرور للوصول إليها.

لوصل مشاركة مجلد أثناء الإقلاع، أضف قيدًا في ملف /etc/fstab؛ على سبيل المثال:

```
//192.168.0.5/share /mnt/windows cifs
auto,username=steve,password=secret,rw 0  0
```

طريقة أخرى لنسخ الملفات من خادوم ويندوز هي استخدام الأداة smbclient؛ فلعرض الملفات في مشاركة ويندوز:

```
smbclient //fs01.example.com/share -k -c "ls"
```

لنسخ ملف من مشاركة، اكتب الأمر:

```
smbclient //fs01.example.com/share -k -c "get file.txt"
```

الأمر السابق سينسخ الملف file.txt إلى مجلد العمل الحالي.

ولنسخ ملف إلى المشاركة:

```
smbclient //fs01.example.com/share -k -c "put /etc/hosts hosts"
```

الأمر السابق سينسخ الملف /etc/hosts إلى //fs01.example.com/share/hosts.

الخيار c- المُستخدَم في الأوامر السابقة يسمح لك بتنفيذ أمر smbclient مباشرةً؛ وهذا يفيد في كتابة السكربتات والعمليات البسيطة على الملفات؛ للدخول إلى مِحَث smb: \> مثل محث FTP حيث تُنفَّذ أوامر لمعالجة الملفات العادية والمجلدات، فنفِّذ الأمر:

```
smbclient //fs01.example.com/share -k
```

ملاحظة: استبدل كل أماكن ورود fs01.example.com، و //192.168.0.5/share، و username=steve,password=secret و file.txt بعنوان IP للخادوم، واسم المشاركة، واسم الملف، واسم المستخدم الحقيقي وكلمة مروره بالقيم الملائمة.

ج. مصادر

- لخياراتٍ إضافية للأمر smbclient، راجع صفحة الدليل man smbclient.
- صفحة دليل man mount.cifs هي أيضًا مرجع مفيد لمعلومات تفصيلية.

١٩

النسخ الاحتياطي

هنالك عدّة طرق لنسخ تثبيت أوبنتو احتياطيًا؛ أهم ما هنالك بالنسبة إلى النسخ الاحتياطية هو تطوير «خطة نسخ احتياطي» تحتوي على ماذا سيُنسَخ احتياطيًّا، وأين سيُنسَخ، وكيف سيُسترجَع.

ستشرح الأقسام الآتية طرقًا مختلفة لإنجاز هذه المهام.

ا. سكربتات شِل

إحدى أبسط الطرق لنسخ نظام احتياطيًّا هي استخدام «سكربت شِل» (shell script)؛ على سبيل المثال، يمكن أن يُستخدَم سكربت لضبط أيّة مجلدات يجب أن تُنسَخ احتياطيًّا، وتُمرَّر هذه المجلدات كوسائط إلى الأداة tar، التي ستُنشِئ ملف أرشيف؛ ويمكن أن يُنقَل ذاك الملف أو ينُسَخ إلى مكانٍ آخر؛ ويمكن أن يُنشَأ أيضًا الأرشيف في نظام بعيد عبر NFS.

الأداة tar تُنشِئ ملف أرشيف واحد من عدّة ملفات أو مجلدات؛ يمكن أيضًا للأداة tar تمرير الملفات عبر أدوات ضغط، وهذا سيؤدي بدوره إلى تقليل حجم ملف الأرشيف.

ا. سكربت شِل بسيط

السكربت الآتي يستخدم tar لإنشاء ملف أرشيف في نظام ملفات NFS موصول عن بعد؛ يُحدَّد اسم الأرشيف باستخدام أدوات إضافية تعمل من سطر الأوامر:

```
#!/bin/sh
####################################
#
# Backup to NFS mount script.
#
####################################

# What to backup.
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# Where to backup to.
dest="/mnt/backup"

# Create archive filename.
day=$(date +%A)
hostname=$(hostname -s)
archive_file="$hostname-$day.tgz"

# Print start status message.
echo "Backing up $backup_files to $dest/$archive_file"
date
echo

# Backup the files using tar.
tar czf $dest/$archive_file $backup_files
# Print end status message.
echo
echo "Backup finished"
date

# Long listing of files in $dest to check file sizes.
ls -lh $dest
```

- ‎$backup_files: متغير يحتوي على قائمة بأيّة مجلدات تود أن تنسخها احتياطيًّا؛ يجب تعديل هذه القائمة لتناسب احتياجاتك.

- ‎$day: متغير يحتوي على اسم اليوم من الأسبوع (مثل Monday، أو Tuesday، أو Wednesday ...إلخ.)؛ وسيُستخدَم لإنشاء ملف أرشيف لكل يوم من الأسبوع، مما يعطي تاريخًا للنسخ الاحتياطي هو سبعة أيام؛ هنالك طرقٌ أخرى للقيام بذلك بما فيها استخدام الأداة date.

- ‎$hostname: متغير يحتوي على الاسم القصير للمضيف؛ استخدام اسم المضيف في اسم ملف الأرشيف يُمكّنك من وضع ملفات الأرشيف اليومية من عدّة خواديم في نفس المجلد.

- ‎$archive_file: الاسم الكامل لملف الأرشيف.

- ‎$dest: الوجهة التي سيُخزَّن فيها ملف الأرشيف؛ يجب أن يكون المجلد موجودًا وفي هذه الحالة موصولًا قبل تنفيذ أمر النسخ الاحتياطي؛ راجع قسم «نظام ملفات الشبكة (NFS)» لمزيدٍ من التفاصيل عن استخدام NFS.

- status messages: الرسائل الاختيارية التي ستُطبَع إلى الطرفية باستخدام الأمر echo.

tar czf $dest/$archive_file $backup_files: أمر tar المُستخدَم لإنشاء ملف الأرشيف.

- الخيار c: إنشاء أرشيف.
- الخيار z: تمرير الملف الناتج عبر الأداة gzip لضغط الأرشيف.
- الخيار f: الإخراج إلى ملف أرشيف؛ عدا ذلك، سيُرسِل الأمر tar مخرجاته إلى مجرى الخرج القياسي.

- ls -lh $dest: عبارة اختيارية تطبع قائمة تفصيلية (-l) بتنسيق سهل القراءة للبشر (-h) لمحتويات مجلد الهدف، هذا الأمر مفيدٌ للتحقق السريع من الحجم التخزيني لملف الأرشيف؛ هذا التحقق ليس بديلًا عن اختبار ملف الأرشيف نفسه!

هذا مثالٌ بسيطٌ عن سكربت شِل للنسخ الاحتياطي؛ لكن هنالك العديد من الخيارات التي يمكن تضمينها في مثل هكذا سكربت، راجع قسم «مصادر» في هذا الفصل للحصول على روابط تُوفِّر معلومات تفصيلية عن كتابة سكربتات شِل.

ب. تنفيذ السكربت

التنفيذ من الطرفية

أبسط طريقة لتنفيذ سكربت النسخ الاحتياطي السابق هي نسخ ولصق محتوياته في ملف باسم backup.sh على سبيل المثال، ثم تنفيذ ما يلي من الطرفية:

```
sudo bash backup.sh
```

هذه طريقة رائعة لاختبار أن كل شيء يعمل على ما يرام في السكربت.

التنفيذ عبر المهام المجدولة (cron)

يمكن استخدام الأداة cron لأتمتة تنفيذ السكربت، يسمح عفريت cron بتنفيذ السكربتات أو الأوامر في أوقات وتواريخ محددة مسبقًا.

يُضبَط cron عبر قيود في ملف crontab؛ تنقسم ملفات crontab إلى حقول:

```
# m h dom mon dow    command
```

- الحقل m: الدقيقة التي سيُنفَّذ عندها الأمر؛ تتراوح القيمة بين ٠ و ٥٩.
- الحقل h: الساعة التي سيُنفَّذ عندها الأمر؛ تتراوح القيمة بين ٠ و ٢٣.
- الحقل dom: يوم الشهر الذي سينُفَّذ عنده السكربت.
- الحقل mon: الشهر الذي سيُنفَّذ عنده السكربت، بين ١ و ١٢.
- الحقل dow: يوم الأسبوع الذي سيُنفَّذ عنده الأمر، تتراوح قيمته بين ٠ و ٧؛ حيث يمكن تحديد يوم الأحد باستخدام ٠ أو ٧، حيث يجوز استخدام كلا القيمتين.
- الحقل command: الأمر الذي سيُنفَّذ.

يجب استخدام الأمر crontab -e لإضافة أو تعديل المدخلات في ملف crontab؛ أيضًا يجب عرض محتويات الملف crontab باستخدام الأمر crontab -l.

أدخِل الأمر الآتي في الطرفية لتنفيذ سكربت backup.sh السابق باستخدام cron:

```
sudo crontab -e
```

ملاحظة: استخدام sudo مع الأمر crontab -e سيُعدِّل جدول المهام للمستخدم الجذر؛ هذا ضروريٌ إذا كنت تنسخ مجلدات احتياطيًا لا يملك وصولًا إليها عدا المستخدم الجذر.

أضف القيد الآتي إلى ملف crontab:

```
# m h dom mon dow   command
0 0 * * * bash /usr/local/bin/backup.sh
```

يجب أن يُنفَّذ سكربت backup.sh كل يوم في تمام الساعة12:00 AM .

ملاحظة: يجب نسخ سكربت backup.sh إلى مجلد /usr/local/bin لكي يعمل القيد السابق عملًا صحيحًا؛ يمكن أن يقبع السكربت في أي مكان في نظام الملفات، وكل ما عليك فعله هو تعديل المسار المذكور في القيد أعلاه بما يلائم مكان وجوده.

ج. الاستعادة من أرشيف

بعد إنشاء الأرشيف، فمن المهم تجربته؛ يمكن أن يُجرَّب الأرشيف بعرض قائمة بالملفات التي يحتويها؛ لكن أفضل طريقة للاختبار هي استعادة ملف من الأرشيف.

يمكنك تنفيذ الأمر الآتي لعرض قائمة بمحتويات الأرشيف:

```
tar -tzvf /mnt/backup/host-Monday.tgz
```

لاستعادة ملف من الأرشيف إلى مجلد مختلف، أدخِل الأمر:

```
tar -xzvf /mnt/backup/host-Monday.tgz -C /tmp etc/hosts
```

يوجه الخيار C- الأمر tar ليستخرج الملفات إلى مجلد محدد؛ حيث سيستخرج الأمر السابق الملف /etc/hosts إلى /tmp/etc/hosts؛ يعيد tar إنشاء هيكلة المجلدات التي تحتوي الملفات.

لاحظ أيضًا أن الشرطة المائلة / في أول المسار قد أزيلت من المسار المُستخرَج إليه.

لاستعادة كل الملفات من الأرشيف، أدخِل الأمرين:

```
cd /
sudo tar -xzvf /mnt/backup/host-Monday.tgz
```

ملاحظة: سيكتب الأمر السابق فوق الملفات في نظام الملفات.

د. مصادر

- للمزيد من المعلومات حول كتابة سكربتات الشِل، راجع «Advanced Bash-Scription Guide».
- كتاب «Teach Yourself Shell Programming in 24 Hours» متوفر على الإنترنت، وهو مصدر ممتاز يشرح كتابة سكربتات الشِل.
- صفحة الويكي «CronHowto» تحتوي على تفاصيل عن خيارات cron المتقدمة.
- راجع دليل GNU tar للمزيد من خيارات tar.
- صفحة ويكيبيديا «Bachup Rotation Scheme» تحتوي على معلومات عن أنماط أخرى للنسخ الاحتياطي.
- يستخدم سكربت الشِل الأداةَ tar لإنشاء الأرشيف، لكن هنالك أدواتٌ سطريةٌ أخرى يمكن استعمالها، على سبيل المثال:
- cpio: يُستخدَم لنسخ الملفات إلى ومن الأرشيفات.
- dd: جزء من حزمة coreutils، الذي هو أداة منخفضة المستوى تستطيع نسخ البيانات من صيغة لأخرى.
- rsnapshot: أداة لأخذ snapshot لنظام الملفات تُستخدَم لإنشاء نسخ من كامل نظام الملفات.
- rsync: أداة مرنة تُستخدَم لإنشاء نسخ تراكمية من الملفات.
- وبالطبع، كتاب «سطر أوامر لينُكس» يحتوي على شرحٍ تفصيلي لأغلبية المواضيع التي ناقشناها ها هنا.

٢. دورة الأرشيف

يسمح السكربت المشروح في القسم الأول من هذا الفصل بسبعة أرشيفات مختلفة فقط؛ ربما يكفي هذا لخادوم لا تتغير البيانات التي فيه كثيرًا؛ أما لو كان يملك الخادوم كميةً كبيرةً من البيانات، فيجب استخدام مخطط معقد للدورات.

ا. دورة أرشيفات NFS

سنعدِّل في هذا القسم السكربت السابق لتطبيق مخطط الجد-الأب-الابن (شهريًا-أسبوعيًا-يوميًا):

- ستُنشَأ نسخ احتياطية يومية من الأحد إلى الجمعة.
- ستُأخذ نسخة احتياطية أسبوعية في يوم السبت مما يمنحك أربع نسخ احتياطية أسبوعية في الشهر.
- ستُأخذ نسخة احتياطية شهرية في أول كل شهر وتكون الدورة شهرين بناءً إذا ما كان رقم الشهر فرديًا أو زوجيًا.

هذا هو السكربت:

```
#!/bin/bash
####################################
#
# Backup to NFS mount script with
# grandfather-father-son rotation.
#
####################################

# What to backup.
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# Where to backup to.
dest="/mnt/backup"

# Setup variables for the archive filename.
day=$(date +%A)
hostname=$(hostname -s)

# Find which week of the month 1-4 it is.
day_num=$(date +%d)
if (( $day_num <= 7 )); then
           week_file="$hostname-week1.tgz"
elif (( $day_num > 7 && $day_num <= 14 )); then
           week_file="$hostname-week2.tgz"
elif (( $day_num > 14 && $day_num <= 21 )); then
           week_file="$hostname-week3.tgz"
elif (( $day_num > 21 && $day_num < 32 )); then
           week_file="$hostname-week4.tgz"
fi

# Find if the Month is odd or even.
month_num=$(date +%m)
month=$(expr $month_num % 2)
if [ $month -eq 0 ]; then
          month_file="$hostname-month2.tgz"
else
          month_file="$hostname-month1.tgz"
fi
```

```
# Create archive filename.
if [ $day_num == 1 ]; then
  archive_file=$month_file
elif [ $day != "Saturday" ]; then
          archive_file="$hostname-$day.tgz"
else
  archive_file=$week_file
fi

# Print start status message.
echo "Backing up $backup_files to $dest/$archive_file"
date
echo

# Backup the files using tar.
tar czf $dest/$archive_file $backup_files

# Print end status message.
echo
echo "Backup finished"
date

# Long listing of files in $dest to check file sizes.
ls -lh $dest/
```

يمكن تنفيذ هذا السكربت بنفس آلية التنفيذ في القسم السابق «تنفيذ السكربت».

عادة جيدة هي أخذ وسائط تخزين النسخ الاحتياطية خارج مكان العمل تحسبًا لوقوع كارثة؛ في مثال سكربت الشِل؛ وسيط التخزين هو خادوم آخر يوفر مشاركة NFS؛ في مثل هذه الحالة، لن يكون خيارًا عمليًا نقل خادوم NFS إلى موقع آخر؛ لكن بناءً على سرعة الاتصال يمكنك نسخ ملف الأرشيف عبر خط WAN إلى خادوم في مكان آخر.

خيار آخر هو نسخ ملف الأرشيف على قرص صلب خارجي يمكن أن يؤخذ بعد ذلك خارج الموقع؛ ولما كانت أسعار الأقراص الصلبة الخارجية تستمر بالانخفاض، فربما يكون ملائمًا استخدام قرصين صلبين لكل مستوى من مستويات الأرشفة؛ هذا سيسمح بوجود قرص صلب خارجي موصول إلى خادوم النسخ الاحتياطي، وآخر في مكانٍ بعيد.

ب. محركات الأشرطة الممغنطة

يمكن استخدام شريط ممغنط (tape) بدلًا من مشاركة NFS، يُسهِّل استخدام الأشرطة الممغنطة دورات الأرشيفات؛ ويجعل أخذ وسائط التخزين خارج الموقع أمرًا هينًا.

القسم الخاص باسم الملف في السكربت لن يكون ضروريًا عند استخدام الأشرطة، لأن البيانات تُرسَل مباشرةً إلى الشريط؛ هنالك حاجة لبعض الأوامر للتعديل على الأشرطة، يتم ذلك باستخدام الأداة mt، التي تُستخدَم للتحكم بالأشرطة الممغنطة وهي جزء من حزمة cpio.

هذا هو سكربت الشِل المعدَّل لاستخدام شريط ممغنط:

```
#!/bin/bash
####################################
#
# Backup to tape drive script.
#
####################################

# What to backup.
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# Where to backup to.
dest="/dev/st0"
```

```
# Print start status message.
echo "Backing up $backup_files to $dest"
date
echo

# Make sure the tape is rewound.
mt -f $dest rewind

# Backup the files using tar.
tar czf $dest $backup_files

# Rewind and eject the tape.
mt -f $dest rewoffl

# Print end status message.
echo
echo "Backup finished"
date
```

ملاحظة: اسم الجهاز الافتراضي لشريط SCSI ممغنط هو /dev/st0؛ استخدم مسار الجهاز الملائم لنظامك في السكربت السابق.

الاستعادة من شريط ممغنط هي نفس عملية الاستعادة من ملف؛ ببساطة أعد لَفّ الشرط واستخدم مسار الجهاز بدلًا من مسار ملف؛ على سبيل المثال، لاستعادة ملف /etc/hosts إلى /tmp/etc/hosts:

```
mt -f /dev/st0 rewind
tar -xzf /dev/st0 -C /tmp etc/hosts
```

٣. برنامج Bacula

إن Bacula هو برنامج للنسخ الاحتياطي يسمح لك بالنسخ والاستعادة والتحقق من البيانات عبر الشبكة؛ هنالك عملاء Bacula للينُكس وويندوز وماك OS X؛ مما يجعله حلًّا متعدد المنصات للنسخ الاحتياطي.

ا. لمحة عن Bacula

يتألف Bacula من عدّة مكونات وخدمات تُستخدَم لإدارة أيّة ملفات لتُنسَخ وأماكن النسخ:

- Bacula Director: خدمة تتحكم بجميع عمليات النسخ الاحتياطي والاستعادة والتحقق والأرشفة.
- Bacula Console: برنامج يسمح بالتواصل مع Director؛ هنالك ثلاثة إصدارات من Console:
  - نسخة نصية تعتمد على سطر الأوامر.
  - واجهة رسومية متناغمة مع غنوم وتَستخدم +GTK.
  - واجهة رسومية تعتمد على wxWidgets.
- Bacula File: ويُعرَف أيضًا بعميل Bacula؛ يُثبَّت هذا التطبيق على الأجهزة التي ستُنسَخ احتياطيًا، وهو مسؤول عن البيانات التي تُطلَب من Director.
- Bacula Storage: التطبيق الذي يجري عملية تخزين واستعادة البيانات من وإلى الوسائط التخزينية.

- Bacula Catalog: مسؤول عن صيانة فهارس الملفات وقواعد بيانات الحجوم لجميع الملفات التي نُسِخَت احتياطيًا، مما يُمكِّن تحديد المكان والاستعادة السريعة للملفات المؤرشفة؛ يدعم Catalog ثلاثة محركات قواعد بيانات مختلفة هي MySQL و PostgreSQL و SQLite.

- Bacula Monitor: يسمح بمراقبة عمل Director، وعفاريت الملفات والتخزين؛ يتوفر Monitor حاليًا كتطبيق +GTK فقط.

يمكن أن تُشغَّل هذه الخدمات والتطبيقات في عدّة خواديم وعملاء، أو يمكن تثبيتها على جهاز واحد إذا كانت ستأخذ نسخةً احتياطيةً لقرص واحد فقط.

ب. التثبيت

ملاحظة: إذا كنت تستخدم MySQL أو PostgreSQL كقاعدة بيانات، فيجب أن تملك أولًا تلك الخدمات؛ إذ لن يثبتها Bacula.

هنالك عدّة حزم تحتوي على مختلف مكونات Bacula، أدخِل الأمر الآتي لتثبيت Bacula:

```
sudo apt-get install bacula
```

يَستخدم التثبيت الافتراضي لحزمة bacula قاعدة بيانات MySQL لتطبيق Catalog؛ إذا أردت استخدام SQLite أو PostgreSQL لتطبيق Catalog، فثبِّت الحزمة bacula-director-sqlite3 أو bacula-director-pgsql على التوالي وبالترتيب.

ستُسأل أثناء التثبيت عن توفير تصاريح لمدير قاعدة البيانات ومالك قاعدة بيانات bacula؛ سيحتاج مدير قاعدة البيانات إلى امتلاك الأذونات الملائمة لإنشاء قاعدة بيانات؛ راجع «الفصل الثاني عشر: قواعد البيانات» لمزيدٍ من المعلومات.

ج. الضبط

ملفات ضبط Bacula منسقة بناءً على «موارد» تشتمل على «تعليمات» محاطة بقوسين معقوفين «{}»؛ ولكل مكون من مكونات Bacula ملف منفصل في مجلد /etc/bacula.

يجب أن تُصرِّح مختلف مكونات Bacula عن نفسها لبعضها بعضًا؛ وهذا يتم باستخدام التعليمة password؛ على سبيل المثال، كلمة مرور مورد Storage في ملف /etc/bacula/bacula-dir.conf يجب أن تُطابِق كلمة مرور Director في /etc/bacula/bacula-sd.conf.

افتراضيًا، تكون هنالك مهمة نسخ احتياطي اسمها Client1 لأرشفة Bacula Catalog؛ إذا كنت تخطط لاستخدام الخادوم للنسخ الاحتياطي لأكثر من عميل، فعليك تعديل اسم هذه المهمة إلى شيء أكثر وصفًا؛ لتغيير الاسم، عدِّل الملف /etc/bacula/bacula-dir.conf:

```
#
# Define the main nightly save backup job
#   By default, this job will back up to disk in
Job {
    Name = "BackupServer"
    JobDefs = "DefaultJob"
    Write Bootstrap = "/var/lib/bacula/Client1.bsr"
}
```

ملاحظة: يغيّر المثال السابق اسم المهمة إلى BackupServer مما يطابق اسم المضيف للخادوم؛ استبدل الكلمة BackupServer باسم المضيف الملائم عندك، أو اسم أكثر وصفًا.

يمكن استخدام Console لإنشاء طلبية لبرمجية Director عن المهام؛ لكن لكي تستخدم Console بمستخدم غير جذر، فيجب أن تضيف المستخدم لمجموعة bacula؛ وذلك بإدخال الأمر الآتي في الطرفية:

```
sudo adduser $username bacula
```

ملاحظة: استبدل $username باسم المستخدم الفعلي؛ وإذا أضفت المستخدم الحالي إلى المجموعة، فعليك تسجيل الخروج ثم إعادة تسجيل الدخول مرةً أخرى لتأخذ الأذونات الجديدة مفعولها.

د. نسخة احتياطية محلية

يشرح هذا القسم كيف تأخذ نسخة احتياطية لمجلدات محددة على مضيف واحد إلى شريط ممغنط محلي.

أولًا، يجب ضبط جهاز Storage؛ وذلك بتعديل /etc/bacula/bacula-sd.conf وإضافة:

```
Device {
    Name = "Tape Drive"
    Device Type = tape
    Media Type = DDS-4
    Archive Device = /dev/st0
    Hardware end of medium = No;
    AutomaticMount = yes;           # when device opened, read
it
    AlwaysOpen = Yes;
    RemovableMedia = yes;
    RandomAccess = no;
    Alert Command = "sh -c 'tapeinfo -f %c | grep TapeAlert'"
}
```

هـذا المثـال يسـتخدم شـريطًا ممغنطًـا مـن نـوع DDS-4؛ عـدِّل قيمـة Media Type و Archive Device لتُطابِق عتادك.

يمكنك أيضًا إزالة التعليق عن أحد الأمثلة في الملف.

بعد تعديل /etc/bacula/bacula-ds.conf، فيجب إعادة تشغيل عفريت Storage:

```
sudo service bacula-sd restart
```

أضف الآن مورد Storage إلى ملف /etc/bacula/bacula-dir.conf لاستخدام الجهاز الجديد:

```
# Definition of "Tape Drive" storage device
Storage {
    Name = TapeDrive
    # Do not use "localhost" here
    Address = backupserver          # N.B. Use a fully
qualified name here
    SDPort = 9103
    Password = "Cv70F6pf1t6pBopT4vQOnigDrR0v3LT3Cgkiyjc"
    Device = "Tape Drive"
    Media Type = tape
}
```

يجب أن تكون قيمة التعليمة Address هي الاسم الكامل للنطاق (FQDN) للخادوم؛ عدِّل backupserver إلى اسم المضيف الحقيقي.

تأكد أيضًا أن التعليمة Password تُطابِق قيمة السلسلة النصية password في ملف /etc/bacula/bacula-sd.conf.

أنشِئ FileSet جديد، الذي سيُحدِّد المجلدات التي ستُأخذ نسخة احتياطية لها، وذلك بإضافة:

```
# LocalhostBacup FileSet.
FileSet {
    Name = "LocalhostFiles"
    Include {
        Options {
        signature = MD5
        compression=GZIP
        }
     File = /etc
     File = /home
    }
}
```

سيُنسخ المجلدان /etc و /home احتياطيًا، تعليمات Options تضبط FileSet لإنشاء بصمة MD5 لكل ملف يُنسَخ احتياطيًا؛ ولضغط الملفات باستخدام gzip.

الآن، أنشِئ Schedule (للجدولة) لمهمة النسخ:

```
# LocalhostBackup Schedule -- Daily.
Schedule {
    Name = "LocalhostDaily"
    Run = Full daily at 00:01
}
```

ستعمل مهمة النسخ الاحتياطي كل يوم في تمام الساعة ٠٠:٠١ أو 12:01 AM؛ تتوفر العديد من خيارات الجدولة الإضافية.

في النهاية، أنشِئ Job:

```
# Localhost backup.
Job {
    Name = "LocalhostBackup"
    JobDefs = "DefaultJob"
    Enabled = yes
    Level = Full
    FileSet = "LocalhostFiles"
    Schedule = "LocalhostDaily"
    Storage = TapeDrive
    Write Bootstrap = "/var/lib/bacula/LocalhostBackup.bsr"
}
```

مما سينسخ نسخةً كاملةً كل يوم إلى الشريط الممغنط.

كل شريط ممغنط مستخدم يجب أن تكون له لافتة (Label)، إذا لم يكن للشريط الحالي لافتةٌ، فسيرسل Bacula بريدًا إلكترونيًا لجعلك تعلم بذلك؛ لضبط لافتة لشريط باستخدام Console، فعليك إدخال الأمر الآتي:

```
bconsole
```

وفي برنامج Bacula Console، أدخِل:

```
label
```

ثم ستُسأل عن مورد Storage:

```
Automatically selected Catalog: MyCatalog
Using Catalog "MyCatalog"
The defined Storage resources are:
     1: File
     2: TapeDrive
Select Storage resource (1-2):2
```

أدخِل اسم الحجم الجديد:

```
Enter new Volume name: Sunday
Defined Pools:
     1: Default
     2: Scratch
```

استبدل Sunday باسمٍ ملائم.

الآن اختر Pool:

```
Select the Pool (1-2): 1
Connecting to Storage daemon TapeDrive at backupserver:9103 ...
Sending label command for Volume "Sunday" Slot 0 ...
```

تهانينا! لقد ضبطت Bacula لنسخ جهازك المحلي احتياطيًا إلى شريط ممغنط.

٥. مصادر

- لمزيد من المعلومات حول خيارات ضبط Bacula، راجع «Bacula User's Manual».
- تحتوي صفحة Bacula الرئيسية على آخر أخبار تطوير Bacula.
- أيضًا، راجع صفحة ويكي أوبنتو «Bacula».

٢٠

الأنظمة الوهمية

يُعتمَد على الأنظمة الوهمية في مختلف البيئات والحالات؛ فلو كنت مطوِّرًا فتوفر لك الأنظمة الوهمية بيئة مُحتوَية حيث تستطيع أن تجري أي نوع من أنواع التطوير دون القلق من تخريب بيئة العمل الرئيسية عندك. وإذا كنت مديرًا للأنظمة، فتستطيع استخدام الأنظمة الوهمية لتعزل خدماتك عزلًا سهلًا وتنقلهم بناءً على الحاجة.

تقنية الأنظمة الوهمية الافتراضية المدعومة في أوبنتو هي KVM، تتطلب KVM ملحقات لدعم الأنظمة الوهمية في عتاد Intel و AMD؛ وتقنية Xen مدعومة أيضًا في أوبنتو؛ حيث يمكن أن تستفيد Xen من تلك الملحقات عند توفرها، لكن يمكن تشغيلها على عتاد دون إضافات الأنظمة الوهمية؛ خيار شائع أخر هو Qemu للعتاد بدون ملحقات الأنظمة الوهمية (virtualization extensions).

ا. مكتبة libvirt

تُستخدَم المكتبة libvirt للتعامل مع مختلف تقنيات الأنظمة الوهمية؛ وقبل البدء مع libvirt، من الأفضل التحقق أنّ عتادك يدعم الملحقات الضرورية لعمل KVM، وذلك بإدخال الأمر الآتي في الطرفية:

```
kvm-ok
```

ستظهر رسالة تعلِمك إن كان معالجك يدعم أو لا يدعم الملحقات العتادية للأنظمة الوهمية.

ملاحظة: يكون من الضروري في أغلب الحواسيب التي تدعم معالجاتها الأنظمة الوهمية أن يفعَّل خيارٌ في BIOS لتمكينها.

ا. التواصل الشبكي الوهمي

هنالك عدّة طرق للسماح لنظام وهمي بالوصول إلى الشبكة الخارجية؛ خيار ضبط التواصل الشبكي الوهمي الافتراضي هو «usermode»، الذي يستخدم بروتوكول SLIRP ويمرِّر التراسل الشبكي عبر NAT عبر بطاقة المضيف إلى الشبكة الخارجية.

لتمكين وصول المضيفين الخارجيين إلى الخدمات مباشرةً على الأنظمة الوهمية، فيجب استخدام ضبط «bridge»؛ هذا يسمح للبطاقات الشبكية الوهمية بالاتصال إلى الشبكة الخارجية عبر البطاقة العتادية، مما يجعلها تبدو كأنها حواسيب عادية لبقية الشبكة.

ب. التثبيت

أدخِل ما يلي في الطرفية لتثبيت الحزم اللازمة:

```
sudo apt-get install kvm libvirt-bin
```

يجب إضافة المستخدم الذي سيدير الآلات الوهمية إلى مجموعة libvirtd بعد تثبيت libvirt-bin؛ وبهذا تعطي المستخدم وصولًا إلى خيارات الشبكة المتقدمة؛ وذلك بإدخال الأمر الآتي:

```
sudo adduser $USER libvirtd
```

ملاحظة: إذا كان المستخدم الذي أضفته هو المستخدم الحالي، فيجب عليك تسجيل الخروج ثم الدخول مرةً أخرى لكي تأخذ عضوية المجموعة الجديدة مفعولها.

أنت الآن جاهز لتثبيت نظام تشغيل «ضيف» (Guest)؛ طريقة تثبيت نظام التشغيل على الآلات الوهمية هي نفس طريقة تثبيته مباشرةً على العتاد؛ أي أنك إما أن تحتاج إلى أتمتة التثبيت، أو إلى لوحة مفاتيح وشاشة موصولين إلى الآلة الفيزيائية.

في حالة الآلات الوهمية، تكون الواجهة الرسومية (GUI) مماثلة لاستخدام لوحة مفاتيح وفأرة فيزيائية؛ فبدلًا من تثبيت واجهة رسومية، يمكن استخدام التطبيق virt-viewer للاتصال إلى الآلة الوهمية باستخدام VNC، راجع القسم «عارض الآلات الوهمية» لمزيدٍ من التفاصيل.

هنالك عدّة طرق لأتمتة تثبيت أوبنتو، إذ يمكن ذلك باستخدام preseed أو kickstart على سبيل المثال. راجع دليل تثبيت أوبنتو للتفاصيل.

طريقة أخرى لتثبيت أوبنتو على آلة افتراضية هي استخدام ubuntu-vm-builder، يسمح ubuntu-vm-builder بإعداد متقدم للأقسام، وتنفيذ سكربتات بعد التثبيت ... إلخ. للتفاصيل، راجع القسم «الصور السحابية وأداة uvtools».

يمكن ضبط Libvirt مع Xen، راجع صفحة مجتمع أوبنتو المُشار إلها في المصادر.

الأداة virt-install

إن virt-install هو جزء من حزمة virtinst، أدخِل الأمر الآتي لتثبيتها:

```
sudo apt-get install virtinst
```

هنالك عدّة خيارات متوفرة عند استخدام virt-install:

```
sudo virt-install -n web_devel -r 256 -disk \
path=/var/lib/libvirt/images/web_devel.img,bus=virtio,size=4 \
-c ubuntu-14.04-server-i386.iso \
--network network=default,model=virtio \
--graphics vnc,listen=0.0.0.0 --noautoconsole -v
```

- الخيار n web_devel-: اسم الآلة الوهمية، سيكون web_devel في هذا المثال.
- الخيار r 256-: تحديد مقدار الذاكرة التي ستستخدمها الآلة الوهمية مقدرًا بالميغابايت.
- الخيار disk path=/var/lib/libvirt/images/web_devel.img,size=4--: الإشارة إلى مسار القرص الوهمي الذي يمكن أن يكون ملفًا أو قسمًا أو حجمًا وهميًا؛ في هذا المثال هنالك ملف باسم web_devel.img في مجلد /var/lib/libvirt/images/ بحجم ٤ غيغابايت، وسيستخدم virtio كناقل للقرص (disk bus).
- الخيار c ubuntu-14.04-server-i386.iso-: الملف الذي سيُستخدَم كقرص CD-ROM وهمي، يمكن أن يكون الملف إما ملف ISO أو مسار إلى جهاز قرص CD-ROM في المضيف.
- الخيار network--: يوفر معلومات حول البطاقة الشبكية للآلة الوهمية؛ يُستخدَم هنا default، وضُبِط موديل البطاقة إلى virtio.
- الخيار graphics vnc,listen=0.0.0.0--: تصدير طرفية الضيف باستخدام VNC على جميع البطاقات الشبكية للمضيف؛ إذ عمومًا لا يكون للخادوم واجهة رسومية، لذلك فيمكن لحاسوب آخر على الشبكة المحلية ذي واجهةٍ رسومية أن يتصل عبر VNC لإكمال التثبيت.

- الخيار noautoconsole--: يؤدي إلى عدم الاتصال تلقائيًا إلى طرفية الآلة الوهمية.
- الخيار v-: إنشاء ضيف وهمي كامل.

بعد تشغيل virt-install يمكنك الاتصال إلى طرفية الآلة الوهمية إما محليًا باستخدام GUI أو باستخدام الأداة virt-viewer.

الأداة virt-clone

يمكن استخدام virt-clone لنسخ آلة وهمية إلى آلة أخرى؛ على سبيل المثال:

```
sudo virt-clone -o web_devel -n database_devel \
-f /path/to/database_devel.img --connect=qemu:///system
```

- o-: الآلة الوهمية الأصلية.
- n-: اسم الآلة الوهمية الجديدة.
- f-: المسار إلى الملف، أو القسم، أو الحجم المنطقي الذي سيُستخدَم من الآلة الوهمية الجديدة.
- connect--: تحديد «المشرف» (hypervisor) الذي سيُتصَّل به.

يمكن أيضًا استخدام الخيار d- أو debug-- لاستكشاف الأخطاء مع virt-clone.

ملاحظة: استبدل web_devel و database_devel بأسماء ملائمة للآلات الوهمية.

ج. إدارة الآلة الوهمية

الأداة virsh

هنالك عدّة أدوات متوفرة لإدارة الآلات الوهمية و libvirt؛ يمكن أن تُستخدَم الأداة virsh من سطر الأوامر؛ هذه بعض الأمثلة:

لعرض قائمة بالآلات الوهمية التي تعمل:

```
virsh -c qemu:///system list
```

لبدء تشغيل آلة وهمية:

```
virsh -c qemu:///system start web_devel
```

وبشكلٍ مشابه، لتشغيل آلة وهمية عند الإقلاع:

```
virsh -c qemu:///system autostart web_devel
```

أعد إقلاع آلة وهمية باستخدام الأمر:

```
virsh -c qemu:///system reboot web_devel
```

يمكن حفظ «حالة» (state) الآلة الوهمية إلى ملف لتُستعاد لاحقًا؛ ما يلي سوف يحفظ حالة الآلة الوهمية إلى ملف مسمى وفقًا لتاريخ اليوم:

```
virsh -c qemu:///system save web_devel web_devel-022708.state
```

ستتوقف الآلة الوهمية عن العمل بعد حفظ حالتها.

يمكن استعادة الآلة الوهمية باستخدام:

```
virsh -c qemu:///system restore web_devel-022708.state
```

نفِّذ الأمر لإيقاف تشغيل آلة وهمية:

```
virsh -c qemu:///system shutdown web_devel
```

يمكن وصل جهاز CD-ROM إلى آلة وهمية بالأمر:

```
virsh -c qemu:///system attach-disk web_devel /dev/cdrom \
/media/cdrom
```

ملاحظة: استبدل في الأمثلة السابقة web_devel مع اسم الآلة الوهمية الملائم، و web_devel-022708.state باسم ملف أكثر وصفًا.

مدير الآلات الوهمية

تحتوي حزمة virt-manager على أداة رسومية لإدارة الآلات الوهمية المحلية والبعيدة؛ أدخِل الأمر الآتي لتثبيتها:

```
sudo apt-get install virt-manager
```

لما كانت الأداة virt-manager تتطلب واجهة رسومية (GUI) فمن المستحسن أن تُثبَّت على محطة عمل أو جهاز للاختبارات بدلًا من خادوم إنتاجي؛ أدخِل الأمر الآتي للاتصال بخدمة libvirt محلية:

```
virt-manager -c qemu:///system
```

تستطيع الاتصال بخدمة libvirt في مضيف آخر بإدخال ما يلي في الطرفية:

```
virt-manager -c qemu+ssh://virtnode1.mydomain.com/system
```

ملاحظة: يفترض المثال السابق أن إمكانية الاتصال عبر SSH بين نظام الإدارة و virtnode1.mydomain.com قد ضُبِطَت مسبقًا، وتستخدم مفاتيح SSH للاستيثاق؛ هنالك حاجة لمفاتيح SSH لأن المكتبة libvirt تُرسِل محث كلمة المرور إلى عملية أخرى. للتفاصيل عن ضبط SSH، راجع «الفصل السادس: الإدارة عن بعد».

د. عارض الآلات الوهمية

يسمح التطبيق virt-viewer لك بالاتصال إلى طرفية الآلة الوهمية لكن virt-viewer يتطلب واجهة رسومية (GUI) للتعامل مع الآلة الوهمية، أدخِل الأمر الآتي من الطرفية لتثبيت virt-viewer:

```
sudo apt-get install virt-viewer
```

بعد تثبيت وتشغيل آلة وهمية، يمكنك الاتصال إلى طرفيتها بالأمر:

```
virt-viewer -c qemu:///system web_devel
```

وكما في virt-manager، يمكن اتصال virt-viewer إلى مضيف بعيد باستخدام SSH مع استيثاق باستخدام مفتاح:

```
virt-viewer -c qemu+ssh://virtnode1.mydomain.com/system \
web_devel
```

تأكد من استبدال web_devel باسم الآلة الوهمية الملائم.

إذا ضبطت استخدام بطاقة شبكية جسرية (bridged network interface)، فيمكنك ضبط وصول SSH إلى الآلة الوهمية؛ راجع الفصل السادس لمزيدٍ من المعلومات.

٥. مصادر

- راجع صفحة KVM الرئيسية للمزيد من التفاصيل.
- للمزيد من المعلومات حول libvirt، انظر إلى صفحة libvirt الرئيسية.
- موقع «Virtual Machine Manager» فيه المزيد من المعلومات حول تطوير virt-manager.
- ادخل إلى قناة ‎#ubuntu-virt على خادوم freenode لمناقشة تقنيات الأنظمة الوهمية في أوبنتو.
- مصدر آخر جيد هو صفحة ويكي أوبنتو «KVM».
- للمزيد من المعلومات حول Xen، بما فيها استخدام Xen مع libvirt؛ رجاءً راجع صفحة ويكي أوبنتو «Xen».

٢. الصور السحابية وأداة uvtool

ا. مقدمة

لما كانت أوبنتو هي أكثر نظام تشغيل مستخدم في العالم في أغلبية المنصات السحابية، فأصبح من الضروري توفير صور سحابية مستقرة وآمنة؛ وفي إصدارة ١٢.٠٤، تحسن استعمال الصور السحابية خارج البنية التحتية للسحابة؛ وأصبح الآن بالإمكان استخدام هذه الصور لإنشاء آلات وهمية دون الحاجة إلى إجراء تثبيت كامل.

ب. إنشاء آلات وهمية باستخدام الأداة uvtool

بدءًا من ١٤.٠٤، أصبح هنالك أداة هي uvtool لتسهيل مهمة توليد الآلات الوهمية (VM) باستخدام الصور السحابية؛ توفر الأداة uvtool آليةً للمزامنة بين الصور السحابية محليًا واستخدامها لإنشاء آلات وهمية في غضون دقائق.

حزم Uvtool

الحزم الآتية واعتمادياتها مطلوبةٌ لاستخدام uvtool:

```
uvtool
uvtool-libvirt
```

تثبيت uvtool مثله كمثل غيره من التطبيقات باستخدام apt-get:

```
sudo apt-get install uvtool
```

هذا سيتثبت الأوامر الرئيسية للأداة uvtool:

- uvt-simplestreams-libvirt
- uvt-kvm

الحصول على صورة سحابة أوبنتو مع uvt-simplestreams-libvirt

هذه إحدى التبسيطات التي جاءت بها الأداة uvtool؛ حيث أنها تعلم أين يمكن العثور على الصور السحابية، لذلك ستحتاج إلى أمرٍ واحد للحصول على صورة سحابية؛ على سبيل المثال، إذا أردت مزامنة كل الصور السحابية لمعمارية amd64، فسيكون الأمر كالآتي:

```
uvt-simplestreams-libvirt sync arch=amd64
```

بعد الفترة الضرورية من الزمن لتنزيل كل الصور من الإنترنت، سيكون لديك مجموعة كاملة من الصور السحابية مخزنةٌ محليًا؛ نفِّذ الأمر الآتي لرؤية الصور التي نُزِّلَت:

```
uvt-simplestreams-libvirt query
release=oneiric arch=amd64 label=release (20130509)
release=precise arch=amd64 label=release (20140227)
release=quantal arch=amd64 label=release (20140302)
release=saucy arch=amd64 label=release (20140226)
release=trusty arch=amd64 label=beta1 (20140226.1)
```

وفي حال أردت مزامنة صورة سحابية واحد محددة، فيمكنك استخدام المُرشِّحات =release و =arch لتعريف الصورة التي يجب مزامنتها:

```
uvt-simplestreams-libvirt sync release=precise arch=amd64
```

إنشاء آلة وهمية باستخدام uvt-kvm

لكي تكون قادرًا على الاتصال بالآلة الوهمية بعد أن تُنشِئها، فمن الضروري أن يكون لديك مفتاح SSH صالح متوفر لمستخدم أوبنتو؛ إذا لم يكن لبيئتك مفتاح، فيمكنك إنشاء واحد بسهولة باستخدام الأمر الآتي:

```
ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ubuntu/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ubuntu/.ssh/id_rsa.
Your public key has been saved in /home/ubuntu/.ssh/id_rsa.pub.
The key fingerprint is:
4d:ba:5d:57:c9:49:ef:b5:ab:71:14:56:6e:2b:ad:9b ubuntu@TrustyS
The key's randomart image is:
+--[ RSA 2048]----+
|               ..|
|              o.=|
|          .    **|
|         +    o+=|
|         S . ...=.|
|          o . .+ .|
|           . . o o |
|              *   |
|             E    |
+-----------------+
```

إنشاء آلة وهمية باستخدام uvtool هو أمر هيّن، ففي أبسط شكل، كل ما عليك فعله هو تنفيذ الأمر:

```
uvt-kvm create firsttest
```

وهذا ما سينُشِئ آلةً وهميةً باسم firsttest باستخدام الصورة السحابية لنسخة الدعم الطويل الحالية (LTS) المتوفرة محليًا، إذا أردت تحديد إصدارة لتُستخدم لإنشاء الآلة الوهمية؛ فستحتاج إلى استخدام مرشح =release:

```
uvt-kvm create secondtest release=trusty
```

يمكن استخدام الأمر uvt-kvm wait NAME للانتظار حتى اكتمال إنشاء الآلة الوهمية:

```
uvt-kvm wait secondttest --insecure
Warning: secure wait for boot-finished not yet implemented; use
--insecure.
```

الاتصال إلى آلة وهمية تعمل

بعد إكمال إنشاء الآلة الوهمية، يمكنك الاتصال إليها عبر SSH:

```
uvt-kvm ssh secondtest --insecure
```

وبالمناسبة، الخيار insecure-- مطلوب، لذلك عليك استخدام هذه الطريقة للاتصال إلى الآلات الوهمية إذا كنت تثق بأمان البنية التحتية لشبكتك تمام الثقة.

يمكنك أيضًا الاتصال إلى الآلة الوهمية باستخدام جلسة ssh اعتيادية باستعمال عنوان IP للآلة الوهمية؛ يمكن أن يُطلَب عنوان IP عبر الأمر الآتي:

```
uvt-kvm ip secondtest
192.168.123.242
ssh -i ~/.ssh/id_rsa ubuntu@192.168.123.242
The authenticity of host '192.168.123.242 (192.168.123.242)'
can't be established.
ECDSA key fingerprint is
3a:12:08:37:79:24:2f:58:aa:62:d3:9d:c0:99:66:8a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.123.242' (ECDSA) to the
list of known hosts.
Welcome to Ubuntu Trusty Tahr (development branch) (GNU/Linux
3.13.0-12-generic x86_64)
 * Documentation:        https://help.ubuntu.com/
 System information disabled due to load higher than 1.0
  Get cloud support with Ubuntu Advantage Cloud Guest:
     http://www.ubuntu.com/business/services/cloud
0 packages can be updated.
0 updates are security updates.
Last login: Fri Mar 21 13:25:56 2014 from 192.168.123.1
```

الحصول على قائمة بالآلات الوهمية التي تعمل

يمكن الحصول على قائمة بالآلات الوهمية التي تعمل على نظامك باستخدام الأمر:

```
uvt-kvm list
secondtest
```

تدمير الآلة الوهمية

بعد أن تنتهي من الآلة الوهمية، يمكنك «تدميرها» والتخلص منها بالأمر:

```
uvt-kvm destroy secondtest
```

المزيد من خيارات uvt-kvm

يمكن أن تُستخدَم الخيارات الآتية لتغيير بعض خصائص الذاكرة الوهمية التي تُنشِئها:

- الخيار memory--: مقدار الذاكرة (RAM) بواحدة الميغابايت، القيمة الافتراضية هي ٥١٢.
- الخيار disk--: مقدار قرص النظام بواحدة الغيغابايت، القيمة الافتراضية هي ٨.
- الخيار cup--: عدد أنوية المعالج، القيمة الافتراضية هي ١.

بعض المعاملات الأخرى لها تأثير على ضبط cloud-init:

- الخيار password password--: السماح بتسجيل الدخول إلى الآلة الوهمية باستخدام حساب ubuntu وكلمة المرور المزودة مع هذا الخيار.
- الخيار script_file run-script-once--: تشغيل السكربت script_file بامتيازات الجذر في أول مرة تُقلِع فيها الآلة الوهمية، لكنه لن يُشغَّل بعد ذلك قط.
- الخيار package_list packages--: تثبيت الحزم المذكورة في package_list والمفصول بينها بفواصل في أول مرة تُقلِع فيها الآلة الوهمية.

يتوفر شرح كامل عن كل الخيارات المتوفرة في صفحة دليل man uvt-kvm.

ج. مصادر

- إذا كنت مهتمًا بتعلم المزيد أو كانت لديك أسئلة أو اقتراحات، فيمكنك مناقشة فريق خادوم أوبنتو على:
  - قناة IRC باسم ubuntu-server# على خادوم Freenode.
  - القائمة البريدية: ubuntu-server at lists.ubuntu.com.

٣. سحابة أوبنتو

الحوسبة السحابية (Cloud Computing) هي نمط حوسبة تسمح بحجز أي مورد من مجموعة واسعة من أنواع الموارد وقت الحاجة؛ هذه الموارد مثل التخزين أو قوة المعالجة أو الشبكة أو البرمجيات يمكن أن تكون مجردة (abstracted) وتوصَّل كخدمة عبر الإنترنت إلى أي مكان في أي وقت. يُدفَع ثمن تلك الخدمات على أساس الوقت المستهلك مثل الخدمات العامة كالكهرباء والمياه وشبكة الهاتف؛ البنية التحتية لسحابة أوبنتو تستخدم البرمجية مفتوحة المصدر OpenStack لبناء حوسبة سحابية قابلة للتوسع للسُحب العامة والخاصة.

ا. التثبيت والضبط

بسبب التواتر العالي لتطوير هذه البرمجية المعقدة، فإننا نُحيل القارئ إلى التوثيق الرسمي لجميع الأمور المتعلقة بتثبيت وضبط هذه البرمجية.

ب. مصادر

- مقالة «Colud Computing – service models».
- OpenStack Compute.
- OpenStack Image Service.
- OpenStack Object Storage Administration Guide.
- مقالة «Installing OpenStack Object Storage on Ubuntu».
- موقع CloudGlossary.com.

٤. حاويات لينُكس LXC

الحاويات (containers) هي تقنية أنظمة وهمية خفيفة؛ حيث تجنح لأن تكون شبيهةً بطريقة chroot محسّنة بدلًا من كونها تقنية أنظمة وهمية كاملة مثل Qemu أو VMware؛ لأن كلاهما لا يحاكي العتاد ولأن الحاويات تشارك نفس نظام التشغيل للمضيف؛ لذلك من الأفضل مقارنة الحاويات إلى «نطاقات سولارس» (Solaris zones) أو «سجون BSD» (BSD jails). إن Linux-vserver و OpenVZ هما نسختان من الحاويات لنظام لينُكس مطورتان بشكل منفصل عن بعضهما؛ في الواقع، ظهرت الحاويات نتيجةً للعمل على تطوير وظائف vserver و OpenVZ.

هنالك نسختان في «مجال المستخدم» (user-space) للحاويات تستخدمان نفس مزايا النواة؛ تسمح Libvirt باستخدام الحاويات عبر محرك LXC بالاتصال إلى «lxc:///»، قد يكون هذا أمرًا ملائمًا لأنها تملك نفس طريقة الاستخدام الموجودة في المحركات الأخرى. النسخة الأخرى المُسماة ببساطة «LXC» هي غير متوافقة مع libvirt؛ لكنها أكثر مرونةً بأدوات أكثر في مجال المستخدم؛ من الممكن التبديل بين النسختين آنفتَيّ الذكر، لكن هنالك بعض الخصوصيات التي قد تسبب ارتباكًا.

سنشرح في هذا الكتاب حزمة lxc شرحًا رئيسيًا، حيث أن استخدام libvirt-lxc ليس مستحسنًا لأنه يفتقر إلى حماية AppArmor لحاويات libvirt-lxc؛ وستكون أسماء الحاويات الموجودة في هذا الفصل هي CN، أو C1، أو C2.

ا. التثبيت

يمكن تثبيت حزمة lxc باستخدام الأمر:

```
sudo apt-get install lxc
```

سنحتاج إلى تنزيل الاعتماديات المطلوبة والمستحسنة، وضبط جسر الشبكة لكي يستخدمه الحاويات؛ إذا أردت استخدام حاويات دون امتيازات، فربما تحتاج إلى أن تتأكد أن للمستخدمِين امتيازات subuids و subgids، وتريد أن تسمح للمستخدمين بوصل الحاويات إلى جسر؛ راجع القسم «الاستخدام الأساسي دون امتيازات».

ب. الاستخدام الأساسي

يمكن أن نستخدم LXC بطريقتين مختلفتين، الأولى بامتيازات عبر تنفيذ أوامر lxc بحساب المستخدم الجذر؛ أو دون امتيازات بتنفيذ أوامر lxc بحساب أي مستخدم عدا الجذر (في الواقع، يمكن تشغيل حاويات دون امتيازات بحساب الجذر، لكننا لن نشرح ذلك هاهنا)؛ الحاويات دون امتيازات محدودة أكثر، فمثلًا لن تستطيع إنشاء عقد أجهزة أو تصل أنظمة ملفات كتلية؛ لكنها أقل خطرًا للمضيف، حيث يكون الجذر في الحاوية مربوطًا بحساب غير جذر في المضيف.

الاستخدام الأساسي بامتيازات

لإنشاء حاوية ذات امتيازات، كل ما عليك فعله هو تنفيذ الأمر:

```
sudo lxc-create --template download --name u1
```

أو بشكل مختصر:

```
sudo lxc-create -t download -n u1
```

الذي سيسألك تفاعليًا عن نوع جذر نظام الملفات لكي يُنزِّل، وخصوصًا التوزيعة والإصدارة والمعمارية؛ يمكنك تحديد هذه القيم في سطر الأوامر لإنشاء حاوية دون الإجابة على تلك الأسئلة تفاعليًا:

```
sudo lxc-create -t download -n u1 -- --dist ubuntu \
--release trusty --arch amd64
```

أو

```
sudo lxc-create -t download -n u1 -- -d ubuntu -r trusty \
-a amd64
```

يمكنك الآن استخدام lxc-ls لعرض قائمة بالحاويات، و lxc-info للحصول على معلومات مفصلة عن حاوية، و lxc-start لبدء و lxc-stop لإيقاف الحاوية؛ بينما يسمح لك الأمران lxc-attach و lxc-console بالدخول إلى حاوية إذا لم يكن الاتصال إليها عبر SSH متاحًا؛ والأمر lxc-destory يحذف الحاوية، بما في ذلك جذر نظام الملفات؛ راجع صفحات الدليل للأوامر السابقة للمزيد من المعلومات؛ أمثلة:

```
sudo lxc-ls --fancy
sudo lxc-start --name u1 --daemon
sudo lxc-info --name u1
sudo lxc-stop --name u1
sudo lxc-destroy --name u1
```

مجالات أسماء المستخدم

تسمح الحاويات دون امتيازات للمستخدمين بإنشاء وإدارة الحاويات دون الحصول على امتيازات الجذر؛ أساس هذه الميزة هو ما يسمى «مجالات أسماء المستخدم» (user namespaces)، إن مجالات أسماء المستخدم هيكليةٌ، حيث تكون المهام ذات امتيازات في مجال الأسماء الأب قادرة على ربط معرِّفاتها إلى مجالات أسماء الأبناء؛ افتراضيًا، كل مهمة على المضيف تعمل في مجال أسماء مبدئي (initial user namespace)، حيث المجال الكامل لمعرفاتها مربوطٌ مع المجال الكامل؛ يمكن مشاهدة ذلك بالنظر إلى /proc/self/uid_map و /proc/self/gid_map؛ اللذان سيظهران القيمة « 0 0 4294967295» عندما يُقرأ من مجال الأسماء المبدئي؛ وفي أوبنتو ١٤.٠٤، المستخدمون الجدد الذين يُنشؤون يكون لهم افتراضيًا مجال من معرفات المستخدم؛ هذه القائمة من المعرفات المُسنَدة يمكن أن تُشاهد في الملفين /etc/subuid و /etc/subgid؛ انظر إلى صفحات الدليل الموافقة لهم للمزيد من المعلومات؛ ويبدأ subuid و subgid عرفيًا من المعرف100000 لتجنب التضارب مع مستخدمي النظام.

إذا أُنشِئ المستخدم في إصدارة قديمة، فيمكنك منحه مجالًا من المعرفات باستخدام usermod، كما يلي:

```
sudo usermod -v 100000-200000 -w 100000-200000 user1
```

برنامجا newuidmap و newgidmap هما برنامجا setuid-root في حزمة uidmap، اللذان يُستخدمان داخليًا بواسطة lxc لربط subuids و subgids من المضيف إلى حاوية دون امتيازات؛ ويتأكدان من أن المستخدم يربط المعرفات المصرَّح بها فقط من ضبط المضيف.

الاستخدام الأساسي دون امتيازات

لإنشاء حاويات دون امتيازات، فإن هنالك خطوات أولية ضرورية؛ حيث تحتاج إلى إنشاء ملف ضبط حاوية افتراضي، مُحدِّدًا ربط المعرفات الذي تريده وضبط الشبكة، بالإضافة إلى ضبط المضيف للسماح لمستخدم دون امتيازات بالارتباط إلى شبكة المضيف؛ يفترض المثال الآتي أنك ربطت معرفات المستخدم والمجموعة ذات المجال100000 - 165536 .

```
mkdir -p ~/.config/lxc
echo "lxc.id_map = u 0 100000 65536" > \
~/.config/lxc/default.conf
echo "lxc.id_map = g 0 100000 65536" >> \
~/.config/lxc/default.conf
echo "lxc.network.type = veth" >> ~/.config/lxc/default.conf
echo "lxc.network.link = lxcbr0" >> ~/.config/lxc/default.conf
echo "$USER veth lxcbr0 2" | sudo tee -a /etc/lxc/lxc-usernet
```

بعد ذلك، يمكنك إنشاء حاويات دون امتيازات بنفس طريقة إنشاء حاويات بامتيازات، لكن ببساطة دون sudo:

```
lxc-create -t download -n u1 -- -d ubuntu -r trusty -a amd64
lxc-start -n u1 -d
lxc-attach -n u1
lxc-stop -n u1
lxc-destroy -n u1
```

التشعب

لكي نشغِّل حاويات داخل حاويات -الأمر الذي يُشار إليه بتشعّب الحاويات- فإن سطرين يجب أن يوجدا في ملف ضبط الحاوية الأب:

```
lxc.mount.auto = cgroup
lxc.aa_profile = lxc-container-default-with-nesting
```

سيسبب السطر الأول بدمج مقبس مدير مجموعات التحكم في الحاوية، لذلك سيكون lxc داخل الحاوية قادرًا على إدارة مجموعات التحكم للحاويات المتشعبة الخاصة به؛ أما السطر الثاني فيسبب تشغيل الحاوية بوضع أكثر سماحيةً بالنسبة إلى AppArmor، مما يسمح للحاوية بإجراء عمليات الوصل اللازمة لبدء تشغيل الحاويات؛ لاحظ أن سياسة AppArmor التي ستُطبَّق أقل أمنًا من السياسة العادية أو سياسة حاوية دون امتيازات؛ راجع القسم «AppArmor» في هذا الفصل لمزيدٍ من المعلومات.

ج. الضبط العام

تُستخدَم ملفات الضبط الآتية من LXC؛ للاستخدام ذو الامتيازات، فإنها ستتواجد في مجلد /etc/lxc، بينما للاستخدام دون امتيازات فستكون موجودةً في ~/.config/lxc/.

lxc.conf يُحدِّد اختياريًا القيم البديلة لمختلف خيارات ضبط lxc، بما فيها lxcpath، والضبط الافتراضي، ومجموعات التحكم التي ستُستخدَم، ونمط إنشاء مجموعة تحكم، وإعدادات الواجهات الخلفية لتخزين lvm و zfs.

default.conf يحدد الضبط الذي يجب أن يحتويه كل ملف ضبط للحاويات المُنشأة حديثًا؛ يحتوي هذا الملف عادةً على الأقل على قسم للشبكة؛ ويحتوي على قسم لربط المعرفات للمستخدمين دون امتيازات.

lxc-usernet.conf يحدد كيف يوصل المستخدمون دون امتيازات حاوياتهم إلى شبكة مملوكة من المضيف.

الملفان lxc.conf و default.conf موجودان في etc/lxc/ و HOME/.config/lxc$؛ بينما الملف lxc-usernet.conf هو ملف لعموم المضيف.

افتراضيًا، تقبع الحاويات في مجلد var/lib/lxc/ بالنسبة للمستخدم الجذر، و HOME/.local/share/lxc$ عدا ذلك؛ يمكن تحديد المسار لجميع أوامر lxc باستخدام المعامل «P|--lxcpath-».

ضبط الشبكة

افتراضيًا، يُنشِئ LXC مجال أسماء شبكي خاص لكل حاوية، الذي يتضمن مجموعة الاتصال الشبكي من الطبقة الثانية (layer 2)، تتصل الحاويات عادةً إلى العالم الخارجي إما بالحصول على بطاقة شبكية فيزيائية، أو عبر نفق veth يُمرَّر إلى الحاوية؛ يُنشِئ LXC جسر NAT، الذي هو lxcbr0 عند إقلاع المضيف؛ والحاويات المُنشَأة باستخدام ملف الضبط الافتراضي سيكون لها بطاقة شبكية veth تكون نهايتها موصولةٌ إلى الجسر lxcbr0، يمكن للبطاقة الشبكية أن تتواجد في مجال أسماء واحد في وقتٍ واحد، لذلك البطاقة الشبكية الفيزيائية المُمررة إلى الحاوية ستكون غير قابلة للاستخدام في المضيف.

من الممكن إنشاء حاويات دون مجال أسماء شبكي خاص، ففي هذه الحالة، ستحصل الحاوية على وصول إلى شبكة المضيف مثل أي تطبيق آخر، لاحظ أنه هذا خطير خصوصًا إذا كانت الحاوية تُشغِّل توزيعة تستخدم upstart، مثل أوبنتو، لأن البرامج التي «تتحدث» إلى init، مثل shutdown، سيتحدثون عبر مقبس مجال يونكس مجرد

(abstract Unix domain socket) إلى upstart للمضيف، مما سيوقف تشغيل المضيف!

لمنح الحاويات في lxcbr0 عنوان IP ثابت بناءً على اسم المضيف، فيمكنك كتابة هذه المدخلات إلى /etc/lxc/dnsmasq.conf:

```
dhcp-host=lxcmail,10.0.3.100
dhcp-host=ttrss,10.0.3.101
```

إذا كان من المطلوب أن يُسمَح بالوصول إلى الحاوية من الخارج، فهنالك عدِّة طرق للالتفاف على ذلك، إحداها هي استخدام iptables لتمرير منافذ المضيف إلى الحاوية، فمثلًا:

```
iptables -t nat -A PREROUTING -p tcp -i eth0 --dport 587 \
-j DNAT --to-destination 10.0.3.100:587
```

طريقة أخرى هي إنشاء جسر إلى إلى البطاقة الشبكية للمضيف (راجع «الفصل الرابع - الشبكات» لمزيدٍ من المعلومات)؛ ثم حدد جسر المضيف في ملف ضبط الحاوية بدلًا من lxcbr0، فمثلًا:

```
lxc.network.type = veth
lxc.network.link = br0
```

في النهاية، يمكنك سؤال LXC ليستخدم macvlan كبطاقة شبكية للحاوية؛ لاحظ أن لهذه الطريقة حدود واعتمادًا على الضبط قد لا تتمكن الحاوية من «التحدث» إلى المضيف نفسه، وبالتالي الخياران السابقان أفضل ويُستخدمان أكثر.

هنالك عدّة طرق لتحديد عنوان IP للحاوية، فأولًا، يمكنك استخدام lxc-ls –fancy الذي سيطبع عناوين IP لجميع الحاويات التي تعمل؛ أو lxc-info -i -H -n C1 الذي سيطبع عنوان IP للحاوية C1؛ إذا كان dnsmasq مثبتًا على المضيف، فيمكنك إضافة قيد إلى /etc/dnsmasq.conf كما يلي:

```
server=/lxc/10.0.3.1
```

بعد أن يستبين dnsmasq عنوان C1.lxc محليًا، فيمكنك تنفيذ:

```
ping C1
ssh C1
```

للمزيد من المعلومات، راجع صفحة دليل lxc.conf ومثال ضبط الشبكة في المسار /usr/share/doc/lxc/examples/.

د. بدء تشغيل LXC

لا يملك LXC عفريتًا يعمل طوال الوقت، لكنه يملك مهام upstart:

- المهمة /etc/init/lxc-net.conf: هي مهمة اختيارية تعمل فقط إذا حَدَّد الملف /etc/default/lxc الخاصية USE_LXC_BRIDGE (قيمتها هي true افتراضيًا)؛ حيث تهيِّء جسر NAT لكي تستخدمه الحاويات.
- المهمة /etc/init/lxc.conf: تعمل إذا كانت الخاصية LXC_AUTO (قيمتها true افتراضيًا) مضبوطة إلى true في /etc/default/lxc؛ حيث تبحث عن القيود في المجلد /etc/lxc/auto/ حيث توجد وصلات رمزية إلى ملفات الضبط للحاويات التي يجب أن تُشغَّل في وقت الإقلاع.
- المهمة /etc/init/lxc-instance.conf: تُستخدَم من /etc/init/lxc.conf للبدء التلقائي لتشغيل حاوية.

ه. التخزين

يدعم LXC عدّة أنماط من التخزين لجذر نظام ملفات الحاوية؛ افتراضيًا يكون مجلدًا بسيطًا، لأنه لا يتطلب أي ضبط مسبق للمضيف طالما أن نظام الملفات فيه مساحة تخزينية كافية؛ وهو لا يتطلب أيضًا امتيازات الجذر لإنشاء المخزن، لذلك سيكون ملائمًا للاستخدام دون امتيازات؛ جذر نظام الملفات للاستخدام مع امتيازات موجود افتراضيًا في المسار /var/lib/lxc/C1/rootfs، بينما جذر نظام الملفات للحاويات التي تعمل دون امتيازات يكون في المسار ~/.local/share/lxc/C1/rootfs، إذا حُدِّد lxcpath خاص في lxc.system.com، فإن جذر نظام ملفات الحاوية سيكون موجودًا في $lxcpath/C1/rootfs.

نسخة snapshot باسم C2 لحاوية C1 التي تُخزَّن في مجلد ستصبح حاوية overlayfs، بجذر نظام ملفات هو overlayfs:/var/lib/lxc/C1/rootfs:/var/lib/lxc/C2/delta0، أنواع التخزين الأخرى تتضمن loop، و btrfs، و LVM، و zfs.

حاوية تعتمد على تخزين btrfs تبدو عمومًا مثل حاوية تعتمد على التخزين في مجلد، ويكون جذر نظام الملفات في نفس المكان؛ لكن جذر نظام الملفات يحتوي على حجم فرعي (subvolume)، لذلك تكون نسخة snapshot مُنشَأة باستخدام نسخة snapshot لحجم فرعي.

جذر نظام الملفات لحاوية تستخدم LVM يمكن أن يكون أي حجم منطقي منفصل؛ اسم مجموعة الحجوم الافتراضي يمكن أن يُحدَّد في ملف lxc.conf؛ ويُضبَط نوع وحجم نظام الملفات لكل حاوية باستخدام lxc-create.

جذر نظام الملفات لحاوية تستخدم zfs هو نظام ملفات zfs منفصل، وموصول في المكان التقليدي /var/lib/lxc/C1/rootfs، يمكن تحديد zfsroot باستخدام lxc-create، ويمكن تحديد قيمة افتراضية في ملف lxc.system.conf.

المزيد من المعلومات حول إنشاء الحاويات بمختلف طرائق التخزين يمكن أن توجد في صفحة دليل lxc-create.

و. القوالب

يتطلب إنشاء حاوية عادةً إنشاء جذر نظام ملفات للحاوية؛ يفوض الأمر lxc-create هذا العمل إلى القوالب (templates)، التي تكون عادةً خاصة بالتوزيعة؛ قوالب lxc التي تأتي مع lxc يمكن أن توجد في مجلد /usr/share/lxc/templates، بما فيها القوالب لإنشاء أوبنتو، ودبيان، وفيدورا، وأوراكل، وسنتوس، وجنتو بالإضافة لغيرها.

إنشاء صور للتوزيعات في أغلب الحالات يتطلب القدرة على إنشاء عقد أجهزة، ويتطلب ذلك أدوات التي ليست متوفرة في بقية التوزيعات، وعادةً يستغرق هذا الأمر وقتًا طويلًا؛ فلذلك يأتي lxc بقالب download، الذي ينزل صور مبنية مسبقًا للحاويات من خادوم lxc مركزي؛ أهم حالة استخدام هي السماح بإنشاء بسيط لحاويات دون امتيازات بواسطة مستخدمين غير الجذر، الذين لن يستطيعوا ببساطة تشغيل الأمر debootstrap.

عند تشغيل lxc-create، فجميع الخيارات التي تأتي بعد «--» تُمرَّر إلى القالب؛ ففي الأمر الآتي، تمرر الخيارات --name و --template و --bdev إلى lxc-create، بينما يمرر الخيار --release إلى القالب:

```
lxc-create --template ubuntu --name c1 --bdev loop -- \
--release trusty
```

يمكنك الحصول على مساعدة حول الخيارات المدعومة في حاوية معينة بتمرير الخيار --help واسم القالب إلى الأمر lxc-create؛ فعلى سبيل المثال، للحصول على مساعدة حول تنزيل قالب:

```
lxc-create --template download --help
```

البدء التلقائي

يدعم LXC تعليم الحاويات لكي تُشغَّل عند إقلاع النظام؛ ففي الإصدارات قبل أوبنتو ١٤.٠٤، كان يتم ذلك باستخدام وصلات رمزية في المجلد /etc/lxc/auto؛ وبدءًا من أوبنتو ١٤.٠٤، يتم ذلك عبر ملفات ضبط الحاوية؛ القيد:

```
lxc.start.auto = 1
lxc.start.delay = 5
```

يعني أن على الحاوية البدء عند إقلاع النظام ويجب الانتظار ٥ ثواني قبل بدء تشغيل الحاوية التالية؛ يدعم LXC أيضًا ترتيب وتجميع الحاويات، وأيضًا إعادة الإقلاع وإيقاف التشغيل عبر مجموعات autostart؛ راجع صفحات دليل lxc-autostart و lxc-container.conf للمزيد من المعلومات.

ز. برمجية AppArmor

يأتي LXC مع ملف ضبط AppArmor مهمته هي حماية المضيف من الإساءة العرضية للامتيازات داخل الحاوية؛ على سبيل المثال، لن تكون الحاوية قادرةً على الكتابة إلى ملف /proc/sysrq-trigger أو أغلبية ملفات /sys.

الملف usr.bin.lxc-start يدخل حيز التنفيذ عند تشغيل lxc-start؛ يمنع ملف الضبط lxc-start من وصل أنظمة ملفات جديدة خارج نظام ملفات الجذر الخاص بالحاوية؛ قبل تنفيذ init للحاوية، فإن LXC يطلب تبديلًا لملف ضبط الحاوية؛ افتراضيًا. هذا الضبط هو السياسة lxc-container-default المعرَّفة في ملف الضبط /etc/apparmor.d/lxc/lxc-default. يمنع هذا الضبط الحاوية من الوصول إلى مسارات خطرة، ومن وصل أغلبية أنظمة الملفات.

لا يمكن تقييد البرامج في الحاوية أكثر من ذلك؛ فعلى سبيل المثال، خادوم MySQL الذي يعمل ضمن نطاق الحاوية (مما يحمي المضيف) لا يمكن أن يدخل في نطاق ملف ضبط MySQL (لحماية الحاوية).

لا يدخل lxc-execute ضمن سلطة AppArmor، لكن الحاوية التي يُنشِئها (spawn) ستكون مقيدةً.

تعديل سياسات الحاوية

إذا وجدت أن lxc-start لا يعمل بسبب تقييد في الوصول من سياسة AppArmor، فيمكنك تعطيل ملف ضبط lxc-start بتنفيذ:

```
sudo apparmor_parser -R /etc/apparmor.d/usr.bin.lxc-start
sudo ln -s /etc/apparmor.d/usr.bin.lxc-start \
/etc/apparmor.d/disabled/
```

هذا سيجعل lxc-start يعمل دون قيود، لكن ستبقى الحدود موجودةً للحاوية نفسها، وإذا أردت إزالة التقييد عن الحاوية، فعليك بالإضافة إلى تعطيل ملف الضبط usr.bin.lxc-start أن تضيف السطر:

```
lxc.aa_profile = unconfined
```

إلى ملف ضبط الحاوية. يأتي LXC مع سياسات بديلة للحاويات، فإذا أردت إنشاء حاويات داخل حاويات (تشعب)، فعليك استخدام ملف الضبط lxc-container-default-with-nasting بإضافة السطر الآتي إلى ملف ضبط الحاوية:

```
lxc.aa_profile = lxc-container-default-with-nesting
```

إذا أردت استخدام libvirt داخل الحاويات، فستحتاج إلى تعديل تلك السياسة (المعرفة في /etc/apparmor.d/lxc/lxc-default-with-nasting) وإزالة التعليق عن السطر الآتي:

```
mount fstype=cgroup -> /sys/fs/cgroup/**,
```

ثم أعد تحميل السياسة.

لاحظ أن سياسة التشعب للحاويات ذات الامتيازات هي أقل أمانًا من السياسة الافتراضية، حيث تسمح للحاويات بإعادة وصل sys/ و proc/ في أماكن غير قياسية، مما يتجاوز سياسة AppArmor؛ لا تملك الحاويات دون امتيازات هذا التأثير الجانبي، لأن جذر الحاوية لا يمكنه الكتابة إلى ملفات proc و sys المملوكة من الجذر.

إذا أردت تشغيل الحاوية بملف ضبط مخصص، فبإمكانك إنشاء ملف ضبط في المسار /etc/apparmor.d/lxc، ويجب أن يبدأ اسمه بالكلمة -lxc لكي يُسمَح لبرنامج lxc-start بالانتقال إليه؛ ملف lxc-default يتضمن إعادة استعمال الملف المجرد في المسار التالي /etc/apparmor.d/abstraction/lxc/container-base؛ طريقة سهلة لإنشاء ملف ضبط جديد هي فعل المثل، ثم إضافة الأذونات الإضافية في نهاية السياسة.

حَمِّل الضبط الجديد بعد إنشاءه كما يلي:

```
sudo apparmor_parser -r /etc/apparmor.d/lxc-containers
```

سيُحمَّل هذا الضبط تلقائيًا بعد إعادة الإقلاع، لأنه يُقرَأ من الملف التالي /etc/apparmor.d/lxc-containers؛ وفي النهاية ولجعل الحاوية CN تستخدم ملف الضبط الجديد lxc-CN-profile، فأضف السطر الآتي إلى ملف الضبط:

```
lxc.aa_profile = lxc-CN-profile
```

ح. مجموعات التحكم

إن مجموعات التحكم (cgroups) هي ميزة من ميزات النواة توفر تجميع للمهام تجميعًا هيكليًا، وإسناد وتحديد الموارد لكل مجموعة تحكم؛ تُستخدَم في الحاويات للحد من الوصول إلى الأجهزة الكتلية أو المحرفية (block or character devices) وتجمّد عمل الحاويات؛ يمكن استعمالها أيضًا لتحديد استخدام الذاكرة وإيقاف الدخل أو الخرج، وضمانة استخدام أصغري للمعالج، والسماح للحاوية بالوصول إلى معالجات محددة.

افتراضيًا، سيُسند للحاوية CN ذات امتيازات مجموعةُ تحكمٍ باسم lxc/CN/؛ وفي حال حدوث تضارب بالاسم (الذي قد يحدث عند استخدام lxcpaths مخصصة)، فستُضاف لاحقة «n-» حيث n هو رقم صحيح يبدأ من الصفر، ويُسنَد إلى اسم مجموعة التحكم.

افتراضيًا، سيُسند للحاوية CN دون امتيازات مجموعة تحكم باسم CN في مجموعة التحكم الخاصة بالمهمة التي بدأت الحاوية، على سبيل المثال usr/1000.user/1.session/CN/ سيُمنَح جذر الحاوية ملكية المجموعة للمجلد (لكن ليس جميع الملفات)، وهذا ما سيسمح بإنشاء مجموعات تحكم فرعية.

وفي أوبنتو ١٤.٠٤، يستخدم LXC مدير مجموعات التحكم cgmanager لإدارة مجموعات التحكم؛ يستقبل مدير مجموعات التحكم طلبات D-Bus عبر مقبس يونكس sys/fs/cgroup/ cgmanager/sock/؛ يجب أن يُضاف السطر الآتي لاستخدام آمن للحاويات المتشعبة:

```
lxc.mount.auto = cgroup
```

إلى ملف ضبط الحاوية، مما يصل المجلد /sys/fs/cgroup/cgmanager وصلًا ترابطيًا (bind-mounted) إلى الحاوية؛ ويجب على الحاوية في المقابل تشغيل وسيط إدارة مجموعات التحكم (ويتم ذلك افتراضيًا إذا كانت الحزمة cgmanager مثبتةً على الحاوية) الذي سينقل المجلد /sys/fs/cgroup/cgmanager إلى /sys/fs/cgroup/cgmanager.lower ثم سيبدأ الاستماع إلى الطلبات للوسيط على مقبسه /sys/fs/cgroup/cgmanager/sock؛ سيتأكد مدير مجموعات التحكم في المضيف أن الحاويات المتشعبة لن تستطيع «الهروب» من مجموعات التحكم المُسندَة إليها أو إنشاء طلبات غير مصرح لها بها.

الاستنساخ

للتزويد السريع بالحاويات، ربما تريد تخصيص حاوية تبعًا لحاجاتك ثم تُنشِئ عدَّة نسخٍ منها؛ ويمكن فعل ذلك بالبرنامج lxc-clone.

الاستنساخ إما أن يكون عبر snapshots أو بنسخ حاوية أخرى؛ فالنسخ هو إنشاء حاوية جديدة منسوخة من الأصلية، وتأخذ مساحة تخزينية مثل الحاوية الأصلية؛ أما snapshot فإنها تستخدم قدرة آلية التخزين على إنشاء snapshots لإنشاء حاوية النسخ-عند-الكتابة (copy-on-write) تُشير إلى الحاوية الأولى؛ يمكن إنشاء snapshots للحاويات المخزنة في btrfs، و LVM، و zfs، وتلك التي تكون مخزنة في مجلدات؛ حيث كل آلية تخزين لها خصوصياتها؛ فمثلًا، حاويات LVM التي ليست thinpool-provisioned لا تدعم إنشاء snapshots من snapshots؛ ولا يمكن حذف حاويات zfs مع snapshots قبل أن تُطلَق (release) جميع snapshots؛ ويجب أن يُخطط جيدًا لحاويات LVM فقد لا يدعم نظام الملفات أن يزيد حجمه. لا يعاني btrfs من تلك السلبيات، لكنه يعاني من أداء fsync منخفض يسبب جعل dpkg و apt-get أبطئ.

تُنشَأ snapshots من الحاويات المخزنة في مجلدات عبر نظام الملفات؛ فمثلًا يكون لحاوية ذات امتيازات C1 جذر نظام ملفات في /var/lib/lxc/C1/rootfs، وستبدأ نسخة snapshot للحاوية C1 باسم C2 بجذر نظام الملفات للحاوية C1 موصولًا للقراءة فقط في /var/lib/lxc/C2/delta0؛ كل ما يهم في هذه الحالة أنه لا يفترض أن تعمل أو تحذف الحاوية C1 أثناء عمل C2؛ من المستحسن اعتبار الحاوية C1 هي حاوية أساسية واستخدام نسخة snapshot لها فقط.

لنفترض أن لدينا حاوية باسم C1، فيمكن إنشاء نسخة منها باستخدام الأمر:

```
sudo lxc-clone -o C1 -n C2
```

يمكن إنشاء snapshot باستخدام:

```
sudo lxc-clone -s -o C1 -n C2
```

راجع صفحة دليل lxc-clone لمزيد من المعلومات.

دعم Snapshots

LXC يدعم snapshots لتسهيل دعم نسخ snapshot لتطوير تكراري للحاوية؛ فعندما تعمل على حاوية C1 -وقبل إنشاء تغيير خطير وصعب العكس- يمكنك إنشاء snapshot:

```
sudo lxc-snapshot -n C1
```

التي هي نسخة snapshot باسم «snap0» في مجلد /var/lib/lxcsnaps أو $HOME/.local/share/lxcsnaps، النسخة الثانية ستُسمى «snap1» وهكذا؛ يمكن عرض النسخ الموجودة حاليًا باستخدام الأمر lxc-snapshot -L -n C1، ويمكن أن تُستعاد نسخة snapshot وتمحى حاوية C1 الحالية باستخدام الأمر lxc-snapshot -r snap1 -n C1، وبعد تنفيذ أمر الاستعادة، فستبقى النسخة snap1 موجودةً.

تُدعَم snapshots لحاويات btrfs، و lvm، و zfs، و overlayfs؛ في حالة إذا استدعي الأمر lxc-snapshot على حاوية تُخزَّن في مجلد، فسيسجل خطأ وستُنشَأ نسخة copy-clone؛ وسبب ذلك أنه لو أنشأ المستخدم نسخة overlayfs snapshot لحاوية تخزن في مجلد، فسينعكس جزء من تغيرات الحاوية الأصلية على نسخة snapshot؛ إذا كنت تريد إنشاء snapshots لحاوية C1 مخزنة في مجلد، فيمكن إنشاء نسخة overlayfs للحاوية C1، ويجب ألّا تلمس C1 بعد ذلك قط، لكن يمكن أن نعدِّل overlayfs وننسخها نسخ snapshots كما نريد، أي:

```
lxc-clone -s -o C1 -n C2
lxc-start -n C2 -d # make some changes
lxc-stop -n C2
lxc-snapshot -n C2
lxc-start -n C2 # etc
```

الحاويات العابرة

«الحاويات العابرة» (Ephemeral containers) هي حاويات تستخدم لمرة واحدة فقط؛ فليكن لدينا حاوية موجودة مسبقًا باسم C1، فيمكنك إنشاء حاوية عابرة باستخدام:

```
lxc-start-ephemeral -o C1
```

ستبدأ الحاوية كنسخة snapshot للحاوية C1، وستطبع التعليمات للدخول إلى الحاوية على الطرفية، وستدمر الحاوية العابرة بعد إيقاف التشغيل، راجع صفحة الدليل lxc-start-ephemeral لمزيد من الخيارات.

ط. إضافات إدارة دورة التشغيل

بدءًا من أوبنتو ١٢.١٠، أصبح من الممكن تعريف إضافات (hooks) تُنفَّذ عند نقاط محددة من دورة تشغيل الحاوية:

الإضافات التي تحدث قبل التشغيل تُنفَّذ من مجال أسماء المضيف قبل أن تُنشَأ طرفيات أو نقاط وصل الحاويات؛ إذا أُجري أي وصل في هذه الفترة، فيجب أن يُنظَّف في إضافة تحدث بعد إيقاف التشغيل.

الإضافات التي تحدث قبل الوصل تُنفَّذ في مجال أسماء الحاوية، لكن قبل أن يوصل جذر نظام الملفات؛ سينظف أي وصل لنظام الملفات في هذه الفترة تلقائيًا عند إيقاف تشغيل الحاوية.

إضافات الوصل هي إضافات تنفذ بعد وصل أنظمة ملفات الحاوية، لكن قبل أن تُنفِّذ الحاوية pivot_root لتغيير جذر نظام ملفاتها.

الإضافات التي تحدث بعد إيقاف التشغيل ستنفَّذ بعد إيقاف تشغيل الحاوية.

إذا أعادت أيّة إضافة خطأً، فسيلغى تشغيل الحاوية، لكن أي إضافة تحدث بعد إيقاف التشغيل ستنفَّذ، ستُسجَّل أيّة مخرجات تولد من السكربت بأولوية التنقيح (debug).

رجاءً راجع صفحة دليل lxc.container.conf لصيغة ملف الضبط التي سيحدد الإضافات؛ يمكن أن تأتي بعض أمثلة الإضافات في الحزمة lxc لتخدم كمثال حول طريقة كتابة إحدى تلك الإضافات.

سطر الأوامر

لدى الحاويات عدد مضبوط من «أسطر الأوامر» (consoles)؛ أحدها موجودٌ دائمًا في /dev/console؛ الذي يظهر في الطرفية عندما تُشغِّل lxc-start ما لم تحدد الخيار d-؛ يمكن إعادة توجيه ناتج خرج /dev/console إلى ملف باستخدام console-file c- في الأمر lxc-start؛ يمكن تحديد عدد إضافي من أسطر الأوامر باستخدام المتغير lxc.tty المضبوط عادةً إلى ٤؛ يمكن أن تظهر أسطر الأوامر تلك في /dev/ttyN (حيث N أكبر أو تساوي ١، وأصغر أو تساوي ٤)؛ ولتسجيل الدخول إلى console 3 من المضيف، فنفِّذ الأمر:

```
sudo lxc-console -n container -t 3
```

إذا لم تحدد الخيار t N-، فسيتم اختيار سطر أوامر غير مُستخدَم؛ للخروج منه، استخدام عبارة الخروج Ctrl-a q؛ لاحظ أن عبارة الخروج لا تعمل في سطر الأوامر الناتج عن lxc-start دون الخيار d-.

ي. استكشاف الأخطاء

التسجيل

إذا حدث شيء ما خاطئ عند تشغيل حاوية، فإن أول خطوة هي الحصول على سجل كامل من LXC:

```
sudo lxc-start -n C1 -l trace -o debug.out
```

هذا سيؤدي إلى جعل lxc يسجل في أعلى درجة إسهاب، التي هي trace، وسيكون ملف التخزين هو ملف باسم «debug.out»، إذا كان الملف debug.out موجودًا مسبقًا، فستُضاف معلومات السجل الجديد إليه.

مراقبة حالة الحاوية

هنالك أمران متوفران لمراقبة تغيرات حالة الحاوية: lxc-monitor الذي يراقب حاويةً أو أكثر لأي تغيرات في الحالة، حيث يأخذ اسم الحاوية مع الخيار n- كالعادة؛ لكن في هذا الحالة، يمكن أن يكون اسم الحاوية تعبيرًا نمطيًا من نمط POSIX للسماح بمراقبة مجموعة من الحاويات؛ يستمر lxc-monitor بالعمل ويعرض تغيرات حالات الحاويات؛ أما lxc-wait فينتظر تغيّرًا محددًا في الحالة ثم ينتهي تنفيذه؛ على سبيل المثال:

```
sudo lxc-monitor -n cont[0-5]*
```

هذا سيعرض جميع تغيرات الحالة لأي حاوية تطابق التعبير النمطي؛ بينما:

```
sudo lxc-wait -n cont1 -s 'STOPPED|FROZEN'
```

سينتظر إلى أن تتغير حالة الحاوية cont1 إلى STOPPED أو FROZEN ثم ينتهي.

الوصل من الممكن في أوبنتو ١٤.٠٤ الوصل (attach) إلى مجال أسماء حاوية، أبسط طريقة هي تنفيذ:

```
sudo lxc-attach -n C1
```

الذي سيبدأ صدفة موصولة لمجال الحاوية C1، أو داخل الحاوية؛ آلية عمل الوصل هي معقدة جدًا، مما يسمح بوصل مجموعة فرعية من مجالات أسماء (namespaces) الحاوية ونمط الحماية (security context)، راجع صفحة الدليل لمزيدٍ من المعلومات.

درجة إسهاب init في الحاوية

إذا أكمل LXC بدء تشغيل الحاوية، لكن فشل إكمال تنفيذ init فيها (على سبيل المثال، لم يُعرَض محث الدخول)، فمن المفيد طلب درجة إسهاب أكبر من عملية init، فلحاوية upstart:

```
sudo lxc-start -n C1 /sbin/init loglevel=debug
```

يمكنك أيضًا بدء تشغيل برامج مختلفة عن init، على سبيل المثال:

```
sudo lxc-start -n C1 /bin/bash
sudo lxc-start -n C1 /bin/sleep 100
sudo lxc-start -n C1 /bin/cat /proc/1/status
```

ك. التعامل مع LXC API

يمكن الوصول إلى غالبية وظائف LXC عبر واجهة برمجية (API) مُصدَّرة من liblxc التي تكون ارتباطاتها متوفرة لعدة لغات برمجية بما فيها بايثون، و lua، وروبي، و go.

ما يلي هو مثال عن استخدام ربط بايثون (المتوفرة في حزمة python3-lxc)، التي تُنشِئ وتبدأ حاوية، ثم تنتظر إلى أن يوقف تشغيلها:

```
sudo python3
Python 3.2.3 (default, Aug 28 2012, 08:26:03)
[GCC 4.7.1 20120814 (prerelease)] on linux2
Type "help", "copyright", "credits" or "license" for more
information.
>>> import lxc
__main__:1: Warning: The python-lxc API isn't yet stable and
may change at any p
oint in the future.
>>> c=lxc.Container("C1")
>>> c.create("ubuntu")
True
>>> c.start()
True
>>> c.wait("STOPPED")
True
```

ل. الحماية

يربط مجال الأسماء المعرفات (ids) إلى الموارد؛ لكنه لا يوفر للحاوية أي معرِّف يمكنه أن يشير إلى المورد، لذلك يمكن أن يُحمى المورد؛ وهذا هو أساس بعض الحماية الموفرة لمستخدمي الحاوية؛ على سبيل المثال، مجال أسماء IPC معزول تمامًا؛ لكن مجالات أسماء أخرى فيها بعض «التسربات» (leaks) التي تسمح للامتيازات بأن تُستخرَج بشكل غير ملائم من الحاوية إلى حاوية أخرى، أو إلى المضيف.

افتراضيًا، تُشغَّل حاويات LXC بسياسة AppArmor التي تقيّد بعض الأفعال، تفاصيل دمج AppArmor مع LXC موجودة في قسم «AppArmor»، الحاويات دون امتيازات تربط الجذر في الحاوية إلى مستخدم دون امتيازات في المضيف، وهذا يمنع الوصول إلى ملفات proc/ و sys/ التي تمثل موارد المضيف، وغيرها من الملفات المملوكة من الجذر في المضيف.

الثغرات في استدعاءات النظام

ميزة أساسية من مزايا الحاويات أنها تشارك النواة مع المضيف؛ وهذا يعني أنه إذا حوت النواة على أيّة ثغرات في استدعاءات النظام (system calls)، فيمكن أن تستغلها الحاوية؛ وبعد أن تتحكم حاوية بالنواة، فيمكنها أن تسيطر سيطرةً كاملةً على أي مورد معروف للمضيف!

بدءًا من أوبنتو ١٢.١٠، يمكن أن تقيَّد الحاوية من مرشِّح seccomp، إن Seccomp هو ميزة جديدة في النواة التي تُرشِّح استدعاءات النظام التي يمكن أن تُستخدَم من المهمة وأولادها؛ بينما يتوقع الوصول إلى إدارة سهلة ومحسنة للسياسة في المستقبل القريب، لكن تحتوي السياسة الحالية على قائمة بيضاء بسيطة لأرقام استدعاءات النظام؛ يبدأ ملف السياسة برقم الإصدار (الذي يجب أن يكون ١) في أول سطر ونوع السياسة (الذي يجب أن يكون whitelist) في ثاني سطر؛ وتُلحَق بقائمة أرقام، كل رقم في سطر.

سنحتاج عادةً لتشغيل حاوية بتوزيعة كاملة إلى عدد كبير من استدعاءات النظام؛ لكن لحاويات البرامج، يمكن أن نقلل عدد استدعاءات النظام المتوفرة إلى رقم قليل؛ وحتى للحاويات التي تشغل توزيعات كاملة يمكن الحصول على فوائد أمنية إذا حذفت -على سبيل المثال- استدعاءات النظام المتوافقة مع ٣٢ بت في حاوية ٦٤ بت؛ راجع صفحة دليل lxc.container.conf للمزيد من التفاصيل حول كيفية ضبط الحاوية لتستخدم seccomp؛ لن تُحمَّل افتراضيًا سياسة seccomp.

م. مصادر

- كتاب «Secure Containers Cookbook» يشرح كيفية استخدام أنماط الحماية لجعل الحاويات أكثر أمانًا.
- مشروع LXC مُستضاف في linuxcontainers.org.
- مشاكل LXC الأمنية مذكورة ومناقشة في صفحة ويكي «LXC Security».

٢١

مجموعات التحكم

مجموعات التحكم هي آلية في النواة لتجميع وتتبع ووضع حد لاستهلاك الموارد للمهام؛ الواجهة الإدارية التي توفرها النواة تكون عبر نظام ملفات وهمي؛ لكن طوِّرت أدوات إدارية لمجموعات التحكم ذات مستوى أعلى، بما فيها libcgroup و lmctfy. بالإضافة لذلك، هنالك دليل في freedesktop.org حول كيف يمكن أن تتعاون التطبيقات بأفضل طريقة باستخدام واجهة نظام الملفات لمجموعات التحكم (cgroup filesystem interface).

في أوبنتو ١٤.٠٤؛ أصبح مدير مجموعات التحكم (cgmanager) متوفرًا كأداة أخرى لإدارة واجهة cgroup؛ حيث هدفه هو الاستجابة لطلبات dbus من أي مستخدم، مما يمكِّنه من إدارة مجموعات التحكم التي أُسنِدَت إليه فقط.

١. لمحة

إن مجموعات التحكم (cgroups) هي الميزة تستعمل لتجميع المهام؛ حيث يكون تتبع الموارد ووضع حدود لها مُدارًا من أنظمة فرعية؛ إذ أنَّ الهيكلية (hierarchy) هي مجموعة من الأنظمة الفرعية الموصولة مع بعضها بعضًا؛ على سبيل المثال، إذا كانت الأنظمة الفرعية للذاكرة والأجهزة (devices) موصولة مع بعضها في /sys/fs/cgroups/set1، فيمكن لأي مهمة في /child1 أن تكون عرضةً للحدود الموافقة للنظامين الفرعيين السابقين.

حيث تُشكِّل كل مجموعة من الأنظمة الفرعية الموصولة «هيكليةً» (مع استثناءات)؛ مجموعات التحكم التي تكون أولاد /child1 تكون عرضةً للحدود المفروضة على /child1، ويكون استهلاك الموارد محسوبًا على /child1.

الأنظمة الفرعية الموجودة تتضمن:

- cpusets: تبسيط إسناد مجموعة من المعالجات وعُقَد الذاكرة إلى مجموعات التحكم؛ فالمهام في مجموعة تحكّم فيها النظام الفرعي cpusets يمكن أن تستخدم المعالجات المُسنَدة إلى تلك المجموعة فقط.
- blkio: تحديد كتل الدخل/الخرج لكل مجموعة تحكم.
- cpuacct: توفير حساب الاستهلاك للمعالج لكل مجموعة تحكم.
- devices: التحكم في قدرة المهام على إنشاء أو استخدام عقد الأجهزة إما باستعمال قائمة بيضاء
- (whitelist) أو سوداء (blacklist).
- freezer: توفير طريقة «لتجميد» (freeze) و «تذويب» (thaw) مجموعات التحكم؛ لا يمكن جدولة
- (scheduled) مجموعات التحكم وهي مجمدة.
- hugetlb: تبسيط وضع حد لاستهلاك hugetlb لكل مجموعة تحكم.
- memory: السماح للذاكرة، وذاكرة النواة، وذاكرة التبديل (swap) بأن تُتَبَّع وتقيّد.

- net_cls: توفير واجهة لوضع علامات على الرزم الشبكية بناءً على مجموعة التحكم المُرسِلة؛ يمكن استعمال هذه العلامات لاحقًا باستخدام tc (traffic controller) لإسناد أولويات للرزم الشبكية.

- net_prio: السماح بضبط أولوية بيانات التراسل الشبكي بناءً على مجموعة التحكم.

- cup: تمكين ضبط جدولة الخصائص على أساس مجموعة التحكم.

- pref_event: تفعيل نمط لكل معالج لمراقبة الخيوط (threads) لمجموعات تحكم معينة.

يمكن إنشاء مجموعات تحكم مُسماة دون استخدام أنظمة فرعية معها، ويكون الغرض من ذلك هو تتبع العمليات؛ على سبيل المثال، يقوم systemd بذلك لتتبع خدماته وجلسات المستخدم.

٢. نظام الملفات

تُنشَأ هيكلية بوصل نسخة من نظام ملفات مجموعة التحكم لكل نظام فرعي مُراد استخدامه كخيار للوصل؛ على سبيل المثال:

```
mount -t cgroup -o devices,memory,freezer cgroup /cgroup1
```

وهذا ما سيُنشِئ هيكلية فوريًا مع الأجهزة ومجموعات التحكم للذاكرة موصولةً مع بعضها؛ ويمكن إنشاء مجموعة تحكم فرعية (child cgroup) باستخدام mkdir:

```
mkdir /cgroup1/child1
```

يمكن نقل المهام إلى مجموعة التحكم الفرعية الجديدة بكتابة أرقام معرفات عملياتهم في ملف tasks أو cgroup.procs:

```
sleep 100
echo $! > /cgroup1/child1/cgroup.procs
```

يمكن الإدارة أيضًا عبر ملفات في مجلدات cgroup؛ على سبيل المثال، لتجميد جميع المهام في child1:

```
echo FROZEN > /cgroup1/child1/freezer.state
```

يمكن العثور على كمية كبيرة من المعلومات عن مجموعات التحكم وأنظمتها الفرعية في مجلد التوثيق cgroups في شجرة مصدر النواة.

٣. التفويض

يمكن لملفات ومجلدات مجموعات التحكم أن تُملَك من مستخدمين غير المستخدم الجذر، مما يمكِّن تفويض (delegation) إدارة مجموعات التحكم؛ عمومًا، تُجبِر النواة القيود المفروضة على الهيكلية على الأولاد؛ على سبيل المثال، إن كانت مجموعة الأجهزة child1/ لا تملك وصولًا للقرص الصلب، فلا تستطيع مجموعة التحكم child1/child2/ إعطاء نفسها هذه الامتيازات.

في أوبنتو ١٤.٠٤، يوضع المستخدمون افتراضيًا في مجموعة من مجموعات التحكم التي يملكونها، مما يسمح لهم باحتواء المهام التي يشغلونها باستخدام مجموعات تحكم فرعية بأمان؛ تُستخدَم هذه الميزة عمليًا ويمكن الاعتماد عليها فمثلًا يمكن استخدامها لإنشاء حاوية LXC دون امتيازات.

٤. المدير

مـــدير مجموعـــات التحكـــم (cgmanager) يـــوفر خدمـــة D-Bus للســـماح للبرامـــج والمستخدمين بإدارة مجموعات التحكم دون الحاجة إلى معرفة أو وصول مباشر إلى نظام ملفات مجموعات التحكم. وللطلبات من المهام في نفس مجال الأسماء (namespace) للمدير، فيمكن للمدير إجراء التحققات الأمنية اللازمة للتأكد من شرعية تلك الطلبات؛ وللطلبات الأخرى، كتلك القادمة من مهمة في حاوية، فيجب القيام بطلبات D-Bus مُحَسَّنة؛ حيث يجب أن تُمرَّر معرفات process، و user، و group على شكل SCM_CREDENTIALS، لذلك يمكن للنواة ربط المعرفات إلى قيم المضيف العامة.

ولتبسيط استخدام استدعاءات D-Bus من جميع المستخدمين، فيبدأ «وسيط مدير مجموعات التحكم» (cgproxy) تلقائيًا في الحاويات؛ حيث يقبل طلبات D-Bus قياسية من المهام في نفس مجال أسمائه، ثم يحوله إلى طلبات SCM D-Bus محسنة التي تُمرَّر بعد ذلك إلى cgmanager.

مثال بسيط عن إنشاء مجموعة تحكم -التي ستُشغِّل تصريفًا (compile) يستهلك كثيرًا من طاقة المعالجة- سيكون كالآتي:

```
cgm create cpuset build1
cgm movepid cpuset build1 $$
cgm setvalue cpuset build1 cpuset.cpus 1
make
```

٥. مصادر

- مشروع cgmanager مُستضاف في linuxcontainers.org.
- صفحة توثيق النواة.
- ويمكن العثور على دليل freedesktop.org لاستخدام مجموعات التحكم.

٢٢

الشبكات العنقودية



‎١. أنظمة DRBD

«جهاز كتلي موزع ومُستنسَخ» (Distributed Replicated Block Device ‏[DRBD]) ينشئ نسخة انعكاسية من الأجهزة الكتلية بين عدّة مضيفين؛ الاستنساخ غير مرئي لبقية التطبيقات على الأنظمة المضيفة. أي أقراص صلبة، أو أقسام، أو أجهزة RAID، أو حجوم منطقية ...إلخ. يمكن أن تُنسَخ انعكاسيًا (mirrored).

للبدء باستخدام DRBD، عليك أولًا تثبيت الحزم الضرورية؛ وذلك بإدخال الأمر الآتي من الطرفية:

```
sudo apt-get install drbd8-utils
```

ملاحظة: إذا كنت تستخدم نواةً وهمية (virtual kernel) كجزءٍ من الآلة الوهمية، فستحتاج إلى تصريف (compile) وحدة debd؛ ربما من الأسهل تثبيت حزمة linux-server داخل الآلة الوهمية. يشرح هذا القسم كيفية ضبط debd لاستنساخ القسم /srv بنظام ملفات ext3 بين مضيفَين؛ لا يهم حجم القسم، لكن يجب أن يكون كلا القسمَين بنفس الحجم.

ا. الضبط

اسم المضيفين في هذا المثال هو debd01 و drbd02؛ وسنحتاج إلى الحصول على خدمة استبيان أسماء إما عبر DNS أو ملف /etc/hosts؛ راجع الفصل الثامن للتفاصيل.

لضبط drbd، عدِّل ملف /etc/drbd.conf على المضيف الأول:

```
global { usage-count no; }
common { syncer { rate 100M; } }
resource r0 {
        protocol C;
        startup {
                wfc-timeout 15;
                degr-wfc-timeout 60;
        }
        net {
                cram-hmac-alg sha1;
                shared-secret "secret";
        }
        on drbd01 {
                device /dev/drbd0;
                disk /dev/sdb1;
                address 192.168.0.1:7788;
                meta-disk internal;
        }
        on drbd02 {
                device /dev/drbd0;
                disk /dev/sdb1;
                address 192.168.0.2:7788;
                meta-disk internal;
        }
}
```

ملاحظة: هنالك خيارات أخرى كثيرة في /etc/drbd.conf، لكن القيم الافتراضية كافيةٌ لهذا المثال.

انسخ الآن الملف /etc/drbd.conf إلى المضيف الثاني:

```
scp /etc/drbd.conf drbd02:~
```

الآن، انسخ الملف إلى /etc في drbd02:

```
sudo mv drbd.conf /etc/
```

باستخدام أداة drbdadm لتهيئة تخزين البيانات الوصفية؛ نفِّذ على كل خادوم ما يلي:

```
sudo drbdadm create-md r0
```

وعلى كلا المضيفين، شغِّل عفريت drbd:

```
sudo service drbd start
```

في drbd01، أو أي مضيف تريد أن يكون هو المضيف الرئيسي، أدخِل ما يلي:

```
sudo drbdadm -- --overwrite-data-of-peer primary all
```

ستبدأ البيانات بالمزامنة مع المضيف الثاني بعد تنفيذ الأمر السابق؛ نفِّذ الأمر الآتي على drbd02 لمشاهدة العملية:

```
watch -n1 cat /proc/drbd
```

اضغط Ctrl+c لإيقاف الأمر السابق.

في النهاية، أضف نظام ملفات إلى dev/drbd0/ وصِله:

```
sudo mkfs.ext3 /dev/drbd0
sudo mount /dev/drbd0 /srv
```

ب. الاختبار

لتختبر إذا كانت الملفات تُزامَن فعليًا بين المضيفين، فانسخ بعض الملفات في drbd01، إلى srv/:

```
sudo cp -r /etc/default /srv
```

ثم افصل srv/:

```
sudo umount /srv
```

الآن نزِّل مرتبة الخادوم الرئيسي إلى دور ثانوي:

```
sudo drbdadm secondary r0
```

ورقّ الخادوم الثانوي إلى رئيسي:

```
sudo drbdadm primary r0
```

ثم صِل القسم:

```
sudo mount /dev/drbd0 /srv
```

وباستخدام ls، يجب أن تشاهد srv/default/ منسوخةً من الخادوم الرئيسي (سابقًا) الذي هو drbd01.

ج. مصادر

- للمزيد من المعلومات حول DRBD، راجع الصفحة الرئيسية الخاصة به.
- تحتوي صفحة دليل man drbd.conf على شرح لخيارات لم نغطها في هذا الفصل.
- راجع أيضًا صفحة الدليل man drbdadm.
- صفحة ويكي أوبنتو «DRBD» فيها المزيد من المعلومات.



خدمة VPN

إن OpenVPN هو حلّ لإنشاء شبكات وهمية خاصة (Virtual Private Networks أو اختصارًا VPN) موجودٌ في مستودعات أوبنتو؛ هو خدمة مرنة وعملية وآمنة، وينتمي إلى عائلة SSL/TLS VPN (التي تختلف عن IPSec VPN)؛ يشرح هذا الفصل تثبيت وضبط OpenVPN لإنشاء شبكة وهمية خاصة.

ا. برمجية OpenVPN

إذا كنت تريد أكثر من مجرد مفاتيح مُشارَكة مسبقًا؛ فيجعل OpenVPN من السهل إعداد واستخدام بينة تحتية للمفتاح العمومي (Public Key Infrastructure اختصارًا PKI) لاستخدام شهادات SSL/TLS للاستيثاق ومبادلة المفاتيح بين خادوم VPN والعملاء؛ يمكن أن يُستخدَم OpenVPN في نمط موَجِّه أو جسر VPN (routed or bridged VPN) ويمكن أن يُضبَط ليستخدم TCP أو UDP؛ ويمكن ضبط رقم المنفذ أيضًا، لكن رقم المنفذ ١١٩٤ هو الرقم الرسمي لهذه الخدمة؛ عملاء VPN موجودون تقريبًا في جميع توزيعات لينُكس، ونظام ماك OS X؛ وويندوز والموجهات (routers) التي تعتمد على OpenWRT.

ا. تثبيت الخادوم

لتثبيت برمجية OpenVPN، أدخِل الأمر الآتي في الطرفية:

```
sudo apt-get install openvpn
```

ب. إعداد البنية التحتية للمفتاح العمومي

أول خطوة لضبط OpenVPN هي إنشاء بنية تحتية للمفتاح العمومي (PKI)؛ التي تحتوي على:

- شهادة منفصلة (تُسمى أيضًا مفتاح عمومي) وشهادة خاصة للخادوم ولكل عميل.
- شهادة سلطة شهادات (CA) رئيسية التي يمكن أن تُستخدَم لتوقيع شهادات كلٍّ من الخادوم والعملاء.

يدعم OpenVPN الاستيثاق ثنائي الاتجاه بناءً على الشهادات، وهذا يعني أن على العميل الاستيثاق من شهادة الخادوم، وعلى الخادوم الاستيثاق من شهادة العميل قبل أن تُنشَأ ثقةٌ مشتركةٌ بينهما.

على الخادوم والعميل الاستيثاق من بعضها أولًا عبر التحقق من أن الشهادة موقعة من سلطة الشهادات الرئيسية، ثم باختبار المعلومات في ترويسة الشهادة المستوثق منها؛ مثل اسم الشهادة الشائع أو نوع الشهادة (عميل أو خادوم).

إعداد سلطة الشهادات

لضبط سلطة شهادات خاصة بك وتوليد شهادات ومفاتيح لخادوم OpenVPN ولبعض العملاء، عليك أولًا نسخ المجلد easy-rsa إلى /etc/openvpn؛ وهذا سيؤكد أن أي تغييرات إلى السكربتات لن تضيع عند تحديث الحزمة؛ أدخِل ما يلي في الطرفية:

```
mkdir /etc/openvpn/easy-rsa/
cp -r /usr/share/easy-rsa/* /etc/openvpn/easy-rsa/
```

الآن عدِّل الملف /etc/openvpn/easy-rsa/vars مغيّرًا ما يلي ليناسب بيئتك:

```
export KEY_COUNTRY="US"
export KEY_PROVINCE="NC"
export KEY_CITY="Winston-Salem"
export KEY_ORG="Example Company"
export KEY_EMAIL="steve@example.com"
export KEY_CN=MyVPN
export KEY_NAME=MyVPN
export KEY_OU=MyVPN
```

أدخِل ما يلي لتوليد شهادة سلطة شهادات رئيسية ومفتاح:

```
cd /etc/openvpn/easy-rsa/
source vars
./clean-all
./build-ca
```

شهادات الخادوم

عليك توليد شهادة ومفتاح خاص للخادوم:

```
./build-key-server myservername
```

وكما في الخطوة السابقة، أغلبية المعاملات يمكن أن تبقى على قيمتها الافتراضية؛ هنالك سؤالان يجب أن تجيب عليهما بالقبول هما " Sign the certificate? [y/n]" و " 1 out of 1 certificate requests certified, commit? [y/n]".

يجب توليد معاملات Diffie Hellman لخادوم OpenVPN:

```
./build-dh
```

جميع الشهادات والمفاتيح ستولد في المجلد الفرعي keys/؛ ومن العادات الشائعة بين المدراء نسخها إلى /etc/openvpn:

```
cd keys/
cp myservername.crt myservername.key ca.crt dh2048.pem \
/etc/openvpn/
```

شهادات العميل

سيحتاج عميل VPN إلى شهادة أيضًا لكي يُعرِّف نفسه إلى الخادوم؛ عليك عادةً إنشاء شهادة منفصلة لكل عميل؛ أدخِل ما يلي في الطرفية لإنشاء شهادة:

```
cd /etc/openvpn/easy-rsa/
source vars
./build-key client1
```

انسخ الملفات الآتية إلى العميل باستخدام طريقة آمنة:

```
/etc/openvpn/ca.crt
/etc/openvpn/easy-rsa/keys/client1.crt
/etc/openvpn/easy-rsa/keys/client1.key
```

ولأن شهادات ومفاتيح العميل مطلوبة فقط على حاسوب العميل، فعليك حذفهم من الخادوم.

ج. ضبط بسيط للخادوم

ستحصل عند تثبيت OpenVPN على أمثلة عن ملفات الضبط:

```
ls -l /usr/share/doc/openvpn/examples/sample-config-files/
total 68
-rw-r--r-- 1 root root 3427 2011-07-04 15:09 client.conf
-rw-r--r-- 1 root root 4141 2011-07-04 15:09 server.conf.gz
```

ابدأ بنسخ وفك ضغط server.conf.gz إلى /etc/openvpn/server.conf.

```
sudo cp /usr/share/doc/openvpn/examples/\
sample-config-files/server.conf.gz /etc/openvpn/
sudo gzip -d /etc/openvpn/server.conf.gz
```

عدِّل ملف /etc/openvpn/server.conf للتأكد من أن الأسطر الآتية تشير إلى الشهادات والمفاتيح التي أنشأتها في القسم السابق:

```
ca ca.crt
cert myservername.crt
key myservername.key
dh dh2048.pem
```

عدِّل الملف /etc/sysctl.conf وأزل التعليق عن السطر الآتي لتفعيل تمرير IP:

```
#net.ipv4.ip_forward=1
```

ثم أعد تحميل sysctl:

```
sudo sysctl -p /etc/sysctl.conf
```

هذا هو الحد الأدنى الذي تحتاج لضبط خادوم OpenVPN؛ يمكنك استخدام جميع الإعدادات الافتراضية في ملف server.conf؛ الآن شغِّل الخادوم، وستجد رسائل التسجيل والخطأ موجودةً في ملف syslog:

```
sudo service openvpn start
 * Starting virtual private network daemon(s)...
   *      Autostarting VPN 'server'
[ OK ]
```

تأكد الآن من أن OpenVPN قد أنشأ البطاقة tun0:

```
ifconfig tun0
tun0      Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-
00-00-00-00-00-00-00
          inet addr:10.8.0.1 P-t-P:10.8.0.2 Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST    MTU:1500
Metric:1
[...]
```

د. ضبط بسيط للعميل

هنالك عدّة نسخ من عملاء OpenVPN بواجهة أو بدون واجهة رسومية؛ يمكنك القراءة المزيد عن العملاء في قسمٍ آخر؛ لكننا الآن سنستخدم عميل OpenVPN في أوبنتو الذي هو نفس الملف التنفيذي للخادوم؛ لذلك عليك تثبيت الحزمة openvpn مرةً أخرى في جهاز العميل:

```
sudo apt-get install openvpn
```

سننسخ هذه المرة ملف مثال الضبط client.conf إلى /etc/openvpn/:

```
sudo cp /usr/share/doc/openvpn/examples/\
sample-config-files/client.conf /etc/openvpn/
```

انسخ مفاتيح العميل والشهادة الصادرين من سلطة الشهادات التي أنشَأتها في قسمٍ سابق، وعدِّل /etc/openvpn/client.conf للتأكد من أن الأسطر الآتية تُشير إلى تلك الملفات؛ يمكنك حذف المسار إذا كانت تلك الملفات موجودةً في /etc/openvpn:

```
ca ca.crt
cert client1.crt
key client1.key
```

وعليك تحديد اسم أو عنوان خادوم OpenVPN واحد على الأقل؛ تأكد أن الكلمة المحجوزة client موجودةٌ في ملف الضبط، لأن هذا ما سيُفعِّل نمط العميل:

```
client
remote vpnserver.example.com 1194
```

شغِّل الآن عميل OpenVPN:

```
sudo service openvpn start
  * Starting virtual private network daemon(s)...
    *     Autostarting VPN 'client'
[ OK ]
```

وتأكد من إنشاء البطاقة الشبكية tun0:

```
ifconfig tun0
tun0    Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-
00-00-00-00-00-00
        inet addr:10.8.0.6      P-t-P:10.8.0.5
Mask:255.255.255.255
        UP POINTOPOINT RUNNING NOARP MULTICAST     MTU:1500
Metric:1
```

وتأكد إن كان بإمكانك عمل ping لخادوم OpenVPN:

```
ping 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
64 bytes from 10.8.0.1: icmp_req=1 ttl=64 time=0.920 ms
```

ملاحظة: يستخدم خادوم OpenVPN أول عنوان IP قابل للاستخدام في شبكة العميل ويكون هذا العنوان هو الوحيد المستجيب للأداة ping؛ على سبيل المثال، لو ضُبِط قناع 24/ لشبكة العميل، فسيقوم باستخدام العنوان 1.؛ عنوان PTP (الند للند، أو peer to peer) الذي تراه في ناتج ifconfig أعلاه لا يجيب عادةً على طلبات ping.

تأكد من جداول التوجيه عندك:

```
sudo netstat -rn
Kernel IP routing table
Destination  Gateway  Genmask         Flags MSS  Window irtt Iface
10.8.0.5     0.0.0.0  255.255.255.255 UH    0    0      0    tun0
10.8.0.1     10.8.0.5 255.255.255.255 UGH   0    0      0    tun0
192.168.42.0 0.0.0.0  255.255.255.0   U     0    0      0    eth0
0.0.0.0      192.168.42.1  0.0.0.0    UG    0    0      0    eth0
```

ه. أول خطوة في استكشاف الأخطاء

إذا لم يعمل ما سبق لك، فعليك أن تفعل ما يلي:

١. تحقق من سجل syslog عندك، أي grep -i vpn /var/log/syslog.
٢. هل يستطيع العميل الاتصال إلى الخادوم؟ ربما يحجب الجدار الناري وصوله؟ تأكد من سجل syslog على الخادوم.
٣. يجب أن يستخدم الخادوم والعميل نفس البروتوكول والمنفذ، مثلًا UDP بمنفذ ١١٩٤؛ راجع خيارَيّ الضبط proto و port.
٤. يجب أن يستخدم الخادوم والعميل نفس إعدادات الضبط الخاصة بالضغط، راجع خيار الضبط comp-lzo.
٥. يجب أن يستخدم الخادوم والعميل نفس الضبط المتعلق بنمط التوجيه والجسور.

و. الضبط المتقدم

ضبط VPN موجّه على الخادوم

الضبط السابق هو ضبط VPN بسيط جدًا، يمكن للعميل الوصول إلى الخدمات على خادوم VPN عبر نفق مشفَّر؛ إذا أردت الوصول إلى المزيد من الخواديم أو أي شيء آخر على الشبكات الأخرى، فأعطي العملاء بعض تعليمات التوجيه؛ على سبيل المثال، لو كان بالإمكان تلخيص شبكة شركتك بالنطاق 192.168.0.0/16؛ فيمكنك إعطاء هذا التوجيه إلى العملاء، لكن عليك أيضًا تغيير التوجيه لطريقة العودة، أي أن خادومك عليه أن يعرف طريقة العودة إلى شبكة عميل VPN.

أو ربما تريد أن تعطي البوابة الافتراضية إلى جميع عملائك وترسل جميع البيانات الشبكية إلى بوابة VPN أولًا، ومن هناك إلى الجدار الناري للشركة ثم إلى الإنترنت؛ يوضح لك هذا القسم بعض الخيارات المتاحة أمامك.

سيسمح إعطاء التوجيهات للعميل له بالوصول إلى شبكات فرعية أخرى خلف الخادوم؛ تذكر أن هذه الشبكات الفرعية يجب أن تعرف أن عليها إعادة توجيه الرزم التابعة لنطاق عناوين عميل OpenVPN ‏(10.8.0.0/24) إلى خادوم OpenVPN.

```
push "route 10.0.0.0 255.0.0.0"
```

ستضبط التعليمة السابقة جميع العملاء كي يعيدوا توجيه بوابة الشبكة الافتراضية عبر VPN، مما يؤدي إلى مرور جميع بيانات الشبكة كتصفح الويب أو طلبات DNS عبر VPN (خادوم OpenVPN أو الجدار الناري المركزي عندك الذي يحتاج إلى تمرير بطاقة TUN/TAP إلى الإنترنت لكي يعمل ذلك عملًا صحيحًا).

اضبط نمط الخادوم ووفر شبكة VPN فرعية لكي يسحب OpenVPN عناوين العملاء منها؛ سيأخذ الخادوم العنوان 10.8.0.1 لنفسه، والبقية ستتوفر للعملاء؛ وكل عميل سيقدر على الوصول إلى الخادوم عبر 10.8.0.1. ضع تعليقًا قبل هذا السطر إذا كنت تستخدم جسر إيثرنت (ethernet bridging):

```
server 10.8.0.0 255.255.255.0
```

حافظ على سجل لارتباطات عناوين IP للعملاء في هذا الملف؛ إذا توقف OpenVPN عن العمل أو أعيد تشغيله، فإن العملاء الذي سيعيدون إنشاء الاتصال سيُسنَد لهم نفس عنوان IP المُسنَد لهم سابقًا.

```
ifconfig-pool-persist ipp.txt
```

أضف خواديم DNS إلى العميل:

```
push "dhcp-option DNS 10.0.0.2"
push "dhcp-option DNS 10.1.0.2"
```

اسمح بالتواصل من العميل إلى العميل:

```
client-to-client
```

تفعيل الضغط على خط VPN:

```
comp-lzo
```

تؤدي التعليمة keepalive بإرسال شبيهة برسائل ping مرارًا وتكرارًا عبر الخط الذي يصل بين الجانبين، لذلك سيعلم كل جانب متى ينقطع الاتصال عن الجانب الآخر؛ السطر الآتي سيرسل ping كل ١ ثانية، بافتراض أن الند البعيد سيكون متوقفًا إذا لم يَرِد رد على الرسالة خلال مدة ٣ ثواني:

```
keepalive 1 3
```

فكرةٌ جيدةٌ هي تقليص امتيازات عفريت OpenVPN بعد التهيئة:

```
user nobody
group nogroup
```

يتضمن OpenVPN 2.0 خاصية تسمح لخادوم OpenVPN بالحصول الآمن على اسم مستخدم وكلمة مرور من العميل المتصل، ويستخدم هذه المعلومات كأساس للاستيثاق بالعميل؛ لاستخدام طريقة الاستيثاق هذه، أولًا أضف تعليمة auth-user-pass إلى ضبط العميل؛ التي ستوجه عميل OpenVPN لطلب اسم مستخدم وكلمة مرور، وتمريرها إلى الخادوم عبر قناة TLS آمنة.

```
# client config!
auth-user-pass
```

هذا سيخبر خادوم OpenVPN أن يتحقق من اسم المستخدم وكلمة المرور المُدخَلة من العملاء باستخدام واحدة PAM لتسجيل الدخول؛ وهذا يفيد في حالة كان عندك آلية مركزية للاستيثاق مثل Kerberos.

```
plugin /usr/lib/openvpn/openvpn-auth-pam.so login
```

ضبط متقدم لخدمة VPN جسرية على الخادوم

يمكن إعداد OpenVPN لكي يعمل بنمط VPN جسري (bridged VPN) أو موجَّه (routed VPN)؛ أحيانًا يُشار لذلك بخدمة VPN تعمل بالطبقة الثانية أو الثالثة من OSI؛ في VPN جسري، جميع الإطارات (frames) الشبكية تكون من الطبقة الثانية (layer-2)، أي جميع إطارات إيثرنت تُرسَل إلى شركاء VPN (VPN partners)؛ بينما تُرسَل الرزم الشبكية من الطبقة الثالثة فقط إلى شركاء VPN (VPN Partners)؛ في النمط الجسري، ستُرسَل جميع البيانات الشبكية بما التي تكون شبيهة بشبكة LAN مثل طلبات DHCP، و طلبات ARP ...إلخ إلى شركاء VPN، لكن في النمط الموجه، سيتم تجاهل تلك الرزم.

٢. تحضير بطاقة شبكية لجسر على الخادوم

تأكد من أن لديك الحزمة bridge-utils:

```
sudo apt-get install bridge-utils
```

قبل أن تضبط OpenVPN في النمط الجسري، عليك تغيير ضبط بطاقات الشبكة؛ لنفترض أن لدى خادومك بطاقة اسمها eth0 موصولة إلى الإنترنت، وبطاقة باسم eth1 موصولة إلى شبكة LAN التي تريد إنشاء جسر لها؛ سيبدو ملف /etc/network/interfaces كما يلي:

```
auto eth0
iface eth0 inet static
    address 1.2.3.4
    netmask 255.255.255.248
    default 1.2.3.1
auto eth1
iface eth1 inet static
    address 10.0.0.4
    netmask 255.255.255.0
```

هذا ضبط بسيط للبطاقة ويجب أن يُعدَّل لكي يغيِّر إلى النمط الجسري حيث تتحول البطاقة eth1 إلى بطاقة br0 الجديدة؛ بالإضافة إلى أننا ضبطنا br0 لتكون البطاقة الجسرية للبطاقة eth1؛ علينا التأكد أن البطاقة eth1 دومًا في نمط تمرير الحزم:

```
auto eth0
iface eth0 inet static
   address 1.2.3.4
   netmask 255.255.255.248
   default 1.2.3.1

auto eth1
iface eth1 inet manual
   up ip link set $IFACE up promisc on

auto br0
iface br0 inet static
   address 10.0.0.4
   netmask 255.255.255.0
   bridge_ports eth1
```

يجب أن تشغِّل الآن تلك البطاقة؛ تحضَّر لأن هذا قد لا يعمل كما هو متوقع، وستفقد التحكم عن بعد؛ تأكد أنك تستطيع حل المشاكل بالوصول إلى الجهاز محليًا.

```
sudo ifdown eth1 && sudo ifup -a
```

٣. إعداد ضبط الخادوم للجسر

عدِّل الملف /etc/openvpn/server.conf، مغيّرًا ما يلي من الخيارات إلى:

```
;dev tun
dev tap
up "/etc/openvpn/up.sh br0 eth1"
;server 10.8.0.0 255.255.255.0
server-bridge 10.0.0.4 255.255.255.0 10.0.0.128 10.0.0.254
```

ثم أنشِئ سكربتًا مساعدًا لإضافة البطاقة tap إلى الجسر، وللتأكد من أن eth1 في وضع تمرير الحزم؛ أنشِئ الملف /etc/openvpn/up.sh:

```
#!/bin/sh

BR=$1
ETHDEV=$2
TAPDEV=$3

/sbin/ip link set "$TAPDEV" up
/sbin/ip link set "$ETHDEV" promisc on
/sbin/brctl addif $BR $TAPDEV
```

ثم اجعل السكربت تنفيذًا:

```
sudo chmod 755 /etc/openvpn/up.sh
```

بعد ضبط الخادوم، عليك إعادة تشغيل خدمة openvpn بإدخال الأمر:

```
sudo service openvpn restart
```

٤. ضبط العميل

أولًا، ثبّت openvpn على العميل:

```
sudo apt-get install openvpn
```

ثم بعد أن يكون الخادوم مضبوطًا، وشهادات العميل منسوخةً إلى /etc/openvpn؛ فأنشِئ ملف ضبط للعميل بنسخ المثال، وذلك بإدخال الأمر الآتي في طرفية جهاز العميل:

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-
files/client.conf /etc/openvpn
```

عدِّل الملف /etc/openvpn/client.conf مغيّرًا الخيارات الآتية:

```
dev tap
;dev tun
ca ca.crt
cert client1.crt
key client1.key
```

في النهاية، أعد تشغيل openvpn:

```
sudo service openvpn restart
```

يجب الآن أن تستطيع الوصول إلى شبكة LAN البعيدة عبر VPN.

ا. نسخ عميل OpenVPN

الواجهة الرسومية لإدارة الشبكة في لينُكس

تأتي أغلبية توزيعات لينُكس بما فيها توزيعة أوبنتو للأجهزة المكتبية على برمجية «مدير الشبكة»، الذي هو واجهة رسومية جميلة لإدارة خيارات الشبكة؛ يمكنك أيضًا إدارة اتصالات VPN منها؛ تأكد أن لديك الحزمة network-manager-openvpn مثبتةً، ستلاحظ هنا أن تثبيتها سيثبِّت حزمًا أخرى مطلوبة:

```
sudo apt-get install network-manager-openvpn
```

لإعلام برمجية «مدير الشبكة» بتثبيت الحزم الجديدة، عليك إعادة تشغيله:

```
restart network-manager
network-manager start/running, process 3078
```

في واجهة مدير الشبكة، اختر لسان VPN واضغط على زر "إضافة"، ثم اختر OpenVPN كنوع خدمة VPN ثم اضغط على «إنشاء»، في النافذة التالية أضف اسم خادوم OpenVPN «كبوابة»، واختر «النوع» إلى «شهادات (TLS)» ثم وجِّه «شهادة المستخدم» إلى شهادتك، و «شهادة CA» إلى سلطة الشهادات التي تعتمدها، و «المفتاح الخاص» إلى ملف مفتاحك الخاص، استخدم الزر «خيارات متقدمة» لتفعيل الضغط أو غيره من الخيارات الخاصة التي ضبطتها على الخادوم؛ جرِّب الآن إنشاء اتصال عبر VPN.

برمجية Tunnelblick لأنظمة ماك OS X

للاتصال بخدمة OpenVPN مع واجهة رسومية يمكنك استخدام Tunnelblick وهو نسخة ممتازة حرة مفتوحة المصدر لواجهة رسومية لعميل OpenVPN لنظام ماك؛ نزِّل آخر نسخة من المثبِّت من الموقع الرسمي وثبتّها؛ ثم ضع ملف الضبط client.ovpn مع الشهادات والمفاتيح سويةً في:

```
/Users/username/Library/ApplicationSupport/Tunnelblick/Configur
ations/
```

ثم شغِّل Tunnelblick من مجلد «التطبيقات» لديك.

```
# sample client.ovpn for Tunnelblick
client
remote blue.example.com
port 1194
proto udp
dev tun
dev-type tun
ns-cert-type server
reneg-sec 86400
auth-user-pass
auth-nocache
auth-retry interact
comp-lzo yes
verb 3
ca ca.crt
cert client.crt
key client.key
```

واجهة رسومية لعميل OpenVPN لويندوز

نـزِّل وثبِّـت آخـر نسـخة مـن عميـل OpenVPN لوينـدوز؛ يمكنـك تثـبيت واجهـة رسـومية اختياريـة باسـم OpenVPN Windows GUI؛ ثـم عليـك تشـغيل خدمـة OpenVPN، وذلـك بالذهاب إلى «ابدأ - جهاز الكومبيوتر - إدارة - الخدمات» و «التطبيقات - الخدمات»، ثم اعـثر على خدمة OpenVPN وشغِّلها، ثم اضبط نمط التشغيل إلى «تلقائي»؛ وعندما تشغِّل OpenVPN MI GUI لأول مرة، فعليك تشغيله كمدير؛ وذلك بالنقر عليه بالزر الأيمن وانتقاء الخيار المناسب.

سيتوجب عليك كتابة ملف ضبط OpenVPN إلى ملف نصي ووضعه في C:\Program Files\OpenVPN\config\client.ovpn مع شهادة CA؛ وعليك وضع شهادة المستخدم في مجلد المنزل للمستخدم كما في المثال الآتي:

```
# C:\Program Files\OpenVPN\config\client.ovpn
client
remote server.example.com
port 1194
proto udp
dev tun
dev-type tun
ns-cert-type server
reneg-sec 86400
auth-user-pass
auth-retry interact
comp-lzo yes
verb 3
ca ca.crt
cert "C:\\Users\\username\\My Documents\\openvpn\\client.crt"
key "C:\\Users\\username\\My Documents\\openvpn\\client.key"
management 127.0.0.1 1194
management-hold
management-query-passwords
auth-retry interact
; Set the name of the Windows TAP network interface device here
dev-node MyTAP
```

وإذا لم ترد الاستيثاق من المستخدم أو كنت تريد تشغيل الخدمة دون تفاعله، فأضف تعليقًا قبل الخيارات الآتية:

```
auth-user-pass
auth-retry interact
management 127.0.0.1 1194
management-hold
management-query-passwords
```

استخدام OpenVPN مع OpenWRT

يوصف OpenWRT أنه توزيعة لينُكس للأجهزة المدمجة مثل موجهات WLAN؛ هنالك بعض الأنواع من تلك الموجهات التي أُعدَّت لتشغيل OpenWRT؛ بالاعتماد على الذاكرة المتوفرة في الموجه لديك، ربما تتمكن من تشغيل برمجيات مثل OpenVPN ويمكنك بناء موجه لمكتب فرعي مع إمكانية الاتصال عبر VPN إلى المكتب الرئيسي.

سجِّل دخولك إلى OpenWRT وثبِّت OpenVPN:

```
opkg update
opkg install openvpn
```

تفقَّد الملف /etc/config/openvpn وضع ضبط العميل هناك؛ وانسخ الشهادة والمفاتيح إلى /etc/openvpn:

```
config openvpn client1
              option enable 1
              option client 1
#             option dev tap
              option dev tun
              option proto udp
              option ca /etc/openvpn/ca.crt
              option cert /etc/openvpn/client.crt
              option key /etc/openvpn/client.key
              option comp_lzo 1
```

أعد تشغيل OpenVPN:

```
service openvpn restart
```

عليك أن ترى إذا كان عليك تعديل إعدادات الجدار الناري والتوجيه في موجهك.

ب. مصادر

- راجع موقع OpenVPN لمزيد من المعلومات.
- راجع كتاب «OpenVPN hardening security guide».
- أيضًا، الكتاب المنشور من Pakt باسم «OpenVPN: Building And Integration Virtual Private Networks» هو مرجع جيد.

٢٤

برمجيات أخرى مفيدة

هنالك العديد من البرمجيات المفيدة جدًا المطورة من فريق خادوم أوبنتو وغيرهم التي تندمج اندماجًا جيدًا مع نسخة خادوم أوبنتو، لكن ربما لا تكون معروفةً جدًا؛ سيعرض هذا الفصل بعض التطبيقات المفيدة التي تسهِّل إدارة خادوم، أو عدّة خواديم، أوبنتو.

ا. تطبيق pam_motd

عندما تسجل دخولك إلى خادوم أوبنتو، ربما تلاحظ «رسالة اليوم» (Message Of The Day اختصارًا MOTD)؛ تأتي هذه المعلومات وتُعرَض من حزمتين:

الحزمة landscape-common: توفر المكتبات الأساسية لبرمجية landscape-client، التي يمكن أن تُستخدَم لإدارة الأنظمة باستخدام تطبيق الويب Landscape؛ تتضمن هذه الحزمة الأداة /usr/bin/landscape-sysinfo التي تُستخدَم لجمع المعلومات التي تُعرَض في MOTD، مثل المعالج، والذاكرة، والمساحة التخزينية للقرص الصلب ...إلخ. على سبيل المثال:

```
System load:          0.0              Processes:
76
Usage of /:           30.2% of 3.11GB  Users logged in:     1
Memory usage:         20%              IP address for eth0:
10.153.107.115
Swap usage:           0%

Graph this data and manage this system at
https://landscape.canonical.com/
```

ملاحظة: يمكنك تشغيل الأمر landscape-sysinfo في أي وقت يدويًا.

حزمة update-notifier-common: التي توفر معلومات عن التحديثات المتوفرة للحزم، والتحققات من أنظمة الملفات (fsck)، ومتى يجب إعادة الإقلاع (مثلًا، بعد تحديث النواة).

تنفِّذ pam_motd السكربتات في /etc/update-motd.d في ترتيبٍ مبنيّ على الرقم الذي يسبق اسم السكربت؛ يُكتَب ناتج السكربتات إلى /var/run/motd، بترتيبٍ رقمي، ثم تُجمَّع مع /etc/motd.tail.

يمكنك إضافة البيانات الديناميكية إلى رسالة اليوم؛ فمثلًا، لإضافة معلومات الطقس المحلي:

أولًا، ثبِّت حزمة weather-util:

```
sudo apt-get install weather-util
```

تستخدم أداة الطقس بيانات METAR من National Oceanic and Atmospheric Administration and Forecast من National Weather Service؛ وللعثور على المعلومات المحلية، فستحتاج إلى رمز ICAO من أربعة محارف؛ الذي يمكن تحديده بتصفح موقع Weather.gov .

وعلى الرغم من أن National Weather Service هي وكالة حكومية تابعة للولايات المتحدة، لكن هنالك محطات طقس متوفرة في جميع أنحاء العالم، لكن ربما لا تتوفر معلومات الطقس لجميع المناطق خارج الولايات المتحدة.

أنشِئ الملف /usr/local/bin/local-weather، الذي هو سكربت شِل بسيط للحصول

على الطقس لمنطقتك المحلية:

```
#!/bin/sh
#
#
# Prints the local weather information for the MOTD.
#
#

# Replace KINT with your local weather station.
# Local stations can be found here:
http://www.weather.gov/tg/siteloc.shtml

echo
weather -i KINT
echo
```

اجعل السكربت قابلًا للتنفيذ:

```
sudo chmod 755 /usr/local/bin/local-weather
```

ثم أنشِئ وصلةً رمزيةً إلى /etc/update-motd.d/98-local-weather:

```
sudo ln -s /usr/local/bin/local-weather \
/etc/update-motd.d/98-local-weather
```

في النهاية، أغلق جلستك الحالية، وأعد تشغيل الدخول لمشاهدة رسالة اليوم الجديدة.

يجب أن يُرحّب بك الآن ببعض المعلومات المفيدة؛ لكن بعض المعلومات حول الطقس المحلي قد لا تكون مفيدةً جدًا! لكن هذا المثال يشرح مرونة pam_motd.

٢. تطبيق etckeeper

يسمح etckeeper بتخزين محتويات /etc/ بسهولة في مستودع نظام تحكم بالإصدارات (VCS)؛ حيث يندمج مع apt لكي يودع التغيرات الحاصلة على /etc تلقائيًّا عندما تُثبَّت أو تُحدَّث الحزم. وضع /etc ضمن مستودع للتحكم بالإصدارات هو أفضل ممارسة يُنصَح بها في مجال العمل، وهدف etckeeper هو جعل هذه المهمة أسهل ما يمكن.

أدخِل الأمر الآتي في الطرفية لتثبيت etckeeper:

```
sudo apt-get install etckeeper
```

ملف الضبط الافتراضي /etc/etckeeper/etckeeper.conf هو بسيط جدًا؛ الخيار الرئيسي يكون لضبط أي متحكم بالإصدارات ليُستخدَم؛ افتراضيًا، يكون etckeeper مضبوط لاستخدام Bazaar للتحكم بالإصدارات؛ ويُهيَّأ المستودع تلقائيًا (ويُودَع فيه لأول مرة) أثناء عملية تثبيت الحزمة؛ من الممكن التراجع عن هذه الخطوة بإدخال الأمر:

```
sudo etckeeper uninit
```

سيودع etckeeper التغيرات غير المودعة التي حصلت على /etc يوميًا افتراضيًا؛ يمكن تعطيل هذا باستخدام خيار الضبط AVOID_DAILY_AUTOCOMMITS؛ وستودع أيضًا التغيرات تلقائيًا قبل وبعد تثبيت الحزم.

للمزيد من القدرة على التحكم بالتغيرات، من المستحسن أن تودع التغيرات يدويًا مع رسالة الإيداع كما يلي:

```
sudo etckeeper commit "..Reason for configuration change.."
```

يمكنك باستخدام أوامر VCS مشاهدة سجل المعلومات حول الملفات في ‎/etc:

```
sudo bzr log /etc/passwd
```

لشرح طريقة الاندماج مع نظام إدارة الحزم، جرِّب تثبيت الحزمة postfix:

```
sudo apt-get install postfix
```

بعد انتهاء التثبيت، ستودَع كل ملفات ضبط postfix إلى المستودع:

```
Committing to: /etc/
added aliases.db
modified group
modified group-
modified gshadow
modified gshadow-
modified passwd
modified passwd-
added postfix
added resolvconf
added rsyslog.d
modified shadow
modified shadow-
added init.d/postfix
added network/if-down.d/postfix
added network/if-up.d/postfix
added postfix/dynamicmaps.cf
added postfix/main.cf
```

```
added postfix/master.cf
added postfix/post-install
added postfix/postfix-files
added postfix/postfix-script
added postfix/sasl
added ppp/ip-down.d
added ppp/ip-down.d/postfix
added ppp/ip-up.d/postfix
added rc0.d/K20postfix
added rc1.d/K20postfix
added rc2.d/S20postfix
added rc3.d/S20postfix
added rc4.d/S20postfix
added rc5.d/S20postfix
added rc6.d/K20postfix
added resolvconf/update-libc.d
added resolvconf/update-libc.d/postfix
added rsyslog.d/postfix.conf
added ufw/applications.d/postfix
Committed revision 2.
```

وكمثال عن طريقة تتبع etckeeper للتغيرات اليدوية، أضف مضيفًا جديدًا إلى ملف /etc/hosts؛ ثم استخدام bzr لمشاهدة أي ملفات قد عُدِّلَت:

```
sudo bzr status /etc/
modified:
hosts
```

يمكنك إيداع التغيرات الآن:

```
sudo etckeeper commit "new host"
```

للمزيد من المعلومات حول bzr، راجع «الفصل السابع عشر: أنظمة التحكم بالإصدارات».

٣. تطبيق Byobu

أحد أكثر البرامج فائدةً لأي مدير أنظمة هو screen، حيث يسمح بتنفيذ عدّة صدفات (shells) في طرفية واحدة؛ ولجعل بعض ميزات screen المتقدمة أكثر قربًا من المستخدم، ولتوفير بعض المعلومات المفيدة عن النظام؛ أنشِئت الحزمة byobu.

عند تنفيذ byobu، سيُظهِر الضغط على زر F9 قائمةَ الضبط التي تسمح لك بما يلي:

- عرض قائمة المساعدة.
- تغيير لون خلفية Byobu.
- تغيير لون أمامية Byobu.
- تبديل ظهور شريط الإشعارات.
- تغيير ربط المفاتيح.
- تغيير سلسلة الخروج.
- إنشاء نوافذ جديدة.
- إدارة النوافذ الافتراضية.

«لا يبدأ Byobu عند تسجيل الدخول (تفعيل ذاك الخيار)».

ربط المفاتيح يحدد بعض الأمور مثل سلسلة الخروج (escape sequence)، وإنشاء نافذة جديدة، وتغيير النافذة...إلخ. هنالك مجموعتا ربط للمفاتيح يمكن الاختيار بينها، واحدة باسم f-keys، والأخرى screen-escape-keys؛ إذا أردت استخدام الربط الافتراضي، فاختر none.

يوفر byobu قائمةً تُظهِر إصدارة أوبنتو، ومعلومات المعالج، ومعلومات الذاكرة، والوقت والتاريخ؛ مما يجعلها تبدو كقائمة سطح مكتب.

تفعيل خيار «لا يبدأ Byobu عند تسجيل الدخول» سيجعل byobu يبدأ عند فتح أي طرفية؛ التغيرات التي تحصل على byobu تكون خاصة بالمستخدم، ولن تؤثر على بقية مستخدمي النظام.

أحد الميزات في byobu هو نمط scrollback، اضغط على زر F7 للدخول بوضع scrollback، الذي يسمح لك بالتنقل إلى المخرجات السابقة باستخدام أوامر شبيهة بأوامر محرر vi؛ هذه قائمة سريعة بأوامر الحركة:

- h: تحريك المؤشر إلى اليسار محرفًا واحدًا.
- j: تحريك المؤشر إلى الأسفل سطرًا واحدًا.
- k: تحريك المؤشر إلى الأعلى سطرًا واحدًا.
- l: تحريك المؤشر إلى اليمين محرفًا واحدًا.
- ٠: تحريك المؤشر إلى بداية السطر الحالي.
- $: تحريك المؤشر إلى نهاية السطر الحالي.
- G: تحريك المؤشر إلى سطر محدد (افتراضيًا إلى النهاية).
- ?: البحث إلى الخلف.
- n: الانتقال إلى المطابقة التالية إما إلى الأمام أو إلى الخلف.

٤. مصادر

- راجع صفحة الدليل man update-motd للمزيد من الخيارات المتوفرة لحزمة update-motd.
- راجع موقع etckeeper لمزيدٍ من التفاصيل حول استخدامه.
- راجع أيضًا صفحة ويكي أوبنتو «etckeeper».
- لآخر الأخبار عن bzr، انظر إلى موقع bzr الرسمي.
- لمزيد من المعلومات حول screen، راجع موقعه الرسمي.
- وأيضًا صفحة ويكي أوبنتو «Screen».
- راجع صفحة مشروع Byobu لمزيدٍ من المعلومات.

الملحق الأول:
التبليغ عن العلل

يستخدم مشروع أوبنتو -وبالتالي نسخة خادوم أوبنتو- موقع Launchpad كمتتبع للعلل؛ ولكي تُسجِّل علّة، فستحتاج إلى حساب في Launchpad، أنشِئ واحدًا إن كان ذلك ضروريًا.

ا. التبليغ عن العلل باستخدام apport-cli

الطريقة المفضّلة للتبليغ عن العلل هي عبر الأمر apport-cli؛ يجب أن يُنفَّذ الأمر على الجهاز المصاب بالعلّة لأنه يجمع معلومات من النظام الذي يُنفَّذ عليه وينشرها إلى البلاغ عن العلة في Launchpad؛ إيصال المعلومات إلى Launchpad قد يصبح صعبًا إن لم يكن يعمل النظام ببيئة سطح مكتب لاستخدام متصفح (وهذا أمرٌ شائعٌ في الخواديم) أو لم يكن يملك وصولًا إلى الإنترنت؛ الخطوات التي يجب اتباعها في هذه الحالات مشروحةٌ في الأسفل.

ملاحظة: يعطي الأمرَين apport-cli و ubuntu-bug نفس النتائج على خادوم بواجهة سطرية؛ حيث الأخير هو فعليًا وصلة رمزية إلى apport-bug، الذي هو ذكي كفايةً لمعرفة إذا كان البيئة المستخدمة هي بيئة سطح مكتب، وسيختار apport-cli فيما عدا ذلك؛ ولمّا كانت أنظمة الخواديم تجنح لأن تكون ببيئة سطرية فقط، فسنشرح في هذا الكتاب apport-cli.

يجب أن تُسجَّل التبليغات عن العلل في أوبنتو على حزمة برمجية محددة، لذلك اسم الحزمة المصابة بالعلة (الحزمة المصدرية أو اسم البرنامج/مساره) يجب أن تُزوِّد إلى apport-cli:

```
apport-cli PACKAGENAME
```

ملاحظة: ارجع إلى «الفصل الثالث: إدارة الحزم» للمزيد من المعلومات حول الحزم في أوبنتو.

بعد انتهاء جمع المعلومات من apport-cli، ستُسأل عمّا تريد فعله بها؛ على سبيل المثال، للتبليغ عن علّة في vim:

```
apport-cli vim
*** Collecting problem information
The collected information can be sent to the developers to
improve the
application. This might take a few minutes.
...
*** Send problem report to the developers?
After the problem report has been sent, please fill out the
form in the automatically opened web browser.
What would you like to do? Your options are:
1 https://launchpad.net/
2 https://help.launchpad.net/YourAccount/NewAccount
    S: Send report (2.8 KB)
    V: View report
    K: Keep report file for sending later or copying to
somewhere else
    I: Cancel and ignore future crashes of this program version
    C: Cancel
Please choose (S/V/K/I/C):
```

أول ثلاثة خيارات مشروحة في الأسفل:

- الخيار Send: إرسال المعلومات المُجمَّعة إلى Launchpad كجزء من عملية إملاء بلاغ علّة جديد؛ ستعطى الفرصة لوصف العلة بكلماتك.

```
*** Uploading problem information
   The collected information is being sent to the bug tracking
system.
   This might take a few minutes.
   94%
   *** To continue, you must visit the following URL:
     https://bugs.launchpad.net/ubuntu/+source/vim/
+filebug/09b2495a-e2ab-11e3-879b-68b5996a96c8?
```

```
 You can launch a browser now, or copy this URL into a browser
on another computer.
   Choices:
       1: Launch a browser now
       C: Cancel
   Please choose (1/C):   1
```

المتصفح الذي سيستخدم عند اختيار «١» هو المتصفح المعروف بالاسم «www-browser» في النظام عبر نظام البدائل الخاص بنظام دبيان (Debian alternatives system)؛ أمثلة عن المتصفحات النصية لتثبيتها تتضمن links، و elinks، و lynx، و w3m؛ يمكنك توجيه متصفح آخر إلى عنوان URL المُعطى.

- الخيار View: عرض المعلومات التي جُمِعَت على الشاشة لمراجعتها؛ التي قد تكون بيانات كثيرة، اضغط على زر «Enter» للتمرير إلى الأسفل، و «q» للخروج والعودة إلى قائمة الاختيار.

- الخيار Keep: كتابة المعلومات المُجمَّعة إلى القرص، يمكن أن يُستخدَم الملف الناتج لاحقًا للتبليغ عن العلة (عمومًا بعد نقل الملف إلى نظام أوبنتو آخر).

```
What would you like to do? Your options are:
        S: Send report (2.8 KB)
        V: View report
        K: Keep report file for sending later or copying to
somewhere else
        I: Cancel and ignore future crashes of this program
version
        C: Cancel
    Please choose (S/V/K/I/C): k
    Problem report file: /tmp/apport.vim.1pg92p02.apport
```

للتبليغ عن العلة، انقل الملف إلى نظام أوبنتو فيه اتصال بالإنترنت ونفِّذ الأمر apport-cli عليه؛ وهذا ما سيسبب إظهار القائمة فوريًا (لأن المعلومات قد جُمِعَت مسبقًا)؛ عليك بعدها أن تضغط على «s» لإرسال البلاغ:

```
apport-cli apport.vim.1pg92p02.apport
```

لحفظ البلاغ إلى القرص مباشرةً (دون الحاجة إلى استخدام القوائم) فيمكنك تنفيذ:

```
apport-cli vim --save apport.vim.test.apport
```

يجب أن تنتهي أسماء ملفات البلاغات باللاحقة ".apport".

ملاحظة: إذا كان النظام الذي فيه اتصال بالإنترنت ليس أوبنتو/دبيان؛ فإن apport-cli ليس متوفرًا، لذلك عليك إنشاء العلة يدويًا؛ لا يجب تضمين بلاغ apport كمرفق بالعلة، لذلك هو عديم الفائدة في هذه الحالة.

---

٢. التبليغ عن الانهيارات في التطبيقات

يمكن ضبط حزمة البرمجيات التي توفر الأداة apport-cli المسماة apport لكي «تلتقط» حالة البرمجيات المنهارة؛ وهذا أمرٌ مفعَّل افتراضيًا (في /etc/default/apport).

سيخزِّن apport نسخةً من تقرير الانهيار في /var/crash بعد أن ينهار التطبيق:

```
-rw-r----- 1 peter whoopsie 150K Jul 24 16:17
↪ _usr_lib_x86_64-linux-gnu_libmenu-cache2_libexec_m
```

استخدم الأداة apport-cli دون أيّة وسائط لمعالجة أيّة تقارير انهيار في الانتظار؛ حيث ستمنحك الخيار للتبليغ عنها واحدةً تلو الأخرى.

```
apport-cli
*** Send problem report to the developers?
After the problem report has been sent, please fill out the
form in the automatically opened web browser.
What would you like to do? Your options are:
   S: Send report (153.0 KB)
   V: View report
   K: Keep report file for sending later or copying to
somewhere else
   I: Cancel and ignore future crashes of this program version
   C: Cancel
Please choose (S/V/K/I/C): s
```

إذا أرسلت البلاغ -كما هو موضَّح في الأعلى- فسيعود إليك محث الطرفية مباشرةً، وسيحتوي المجلد /var /crash على ملفين إضافيين:

```
-rw-r----- 1 peter    whoopsie 150K Jul 24 16:17
↪ _usr_lib_x86_64-linux-gnu_libmenu-cache2_libexec_m
-rw-rw-r-- 1 peter    whoopsie    0 Jul 24 16:37
↪ _usr_lib_x86_64-linux-gnu_libmenu-cache2_libexec_m
-rw------- 1 whoopsie whoopsie    0 Jul 24 16:37
↪ _usr_lib_x86_64-linux-gnu_libmenu-cache2_libexec_m
```

إرسال بلاغ الانهيار بهذه الطريقة لن يسبب في إنشاء بلاغ عام (public) للعلة؛ سيكون البلاغ خاصًا (private) في Launchpad، هذا يعني أنه سيكون مرئيًا لجزءٍ من الناشطين في تتبع العلل؛ حيث سيبحثون عن أيّة معلومات خاصة بك قبل إنشاء بلاغ عام.

٣. مصادر

- راجع صفحة ويكي أوبنتو «Reporting Bugs».
- صفحة «Apport» فيها بعض المعلومات المفيدة، وتشير بعضها إلى كيفية استخدام الواجهة الرسومية للتبليغ عن العلل.